Privacy Policy & Procedure

Statement
St Giles, ARC Support Services and ASELCC (known as the Organisation hereinafter) is committed to managing personal information in accordance with the Australian Privacy Principles under the Privacy Act 1988 (Cth) and in accordance with other applicable privacy laws.

This document sets out the Organisation's Policy and Procedure for managing personal information collected, stored, used, disclosed and otherwise managed by the Organisation for any individual within the Organisation.

Purpose and Scope
To ensure all staff have an understanding of the Organisation's requirements relating to the collection, storage, use and disclosure of all personal information of our participants, staff, and stakeholders in accordance with privacy laws.

Definitions and Acronyms
Privacy – the state of being free from public attention.

Confidentiality – the state of keeping or being kept private.

Confidential Information - includes, but is not limited to, documentation or information received in the performance of duties as well as confidential information, records, materials, trade secrets, financial and business information and activities and personal details of the participants of the Organisation and of the Organisation itself.

Employees - People who are paid wages or salary by the Organisation to perform duties.

Personal Information – information or an opinion about an individual whose identity is reasonable identifiable. Examples of personal information include a person' name, address, date of birth and details about their health.

Staff - People who perform duties as directed by an organisation. Staff include employees, volunteers and contractors.

Amendments
This policy will be reviewed and updated on an as-needed basis with a minimum of every five years; input is encouraged from Board members, employees and volunteers to advise the Organisation's Quality Manager of any changes required.

Responsibilities
It is the responsibility of Board members, casual, permanent and contract employees and volunteers to adhere to the Privacy Policy and Procedure at all times.

Policy
What information does the Organisation collect?
Participants and Prospective Participants
When a prospective participant enquires about the Organisation's services or when a participant commences services with the Organisation, a record is made which includes the individual's personal information.

The type of personal information that the Organisation collects will vary depending on the circumstances of collection and the kind of service that the participant requests from the Organisation, but will typically include:

- participant name, e-mail, postal address and other contact details;
- information about the individual's employer or an organisation who the individual represents;
- information about the services the participant requires

- professional details; and
- any additional personal information the participant provides to the Organisation, or authorises the Organisation to collect, as part of the participant's interaction with the Organisation.

Prospective Employees or Applicants
The Organisation collects personal information when recruiting personnel, such as name, contact details, qualifications and work history. Generally, the Organisation will collect this information directly from the applicant.

The Organisation may also collect personal information from third parties in ways which you would expect (for example, from recruitment agencies or referees nominated by the applicant). Before offering a position, the Organisation may collect additional details such as the applicant's tax file number and superannuation information and other information necessary to conduct background checks to determine the applicant's suitability for certain positions, for example - positions which involve working with children.

Other Individuals
The Organisation may collect personal information about other individuals who are not participants of the Organisation. This includes customers and members of the public who participate in events the Organisation is involved with, individual service providers and contractors to the Organisation, and other individuals who interact with the Organisation on a commercial basis. The kinds of personal information collected will depend on the capacity in which the individual is dealing with the Organisation. Generally, it would include the individual's name, contact details, and information regarding the Organisation's interactions and transactions with the individual.
If the individual is participating in an event that the Organisation is managing or delivering, the Organisation may take images or audio-visual recordings which identifies the individual.

In limited circumstances, the Organisation may collect information which is considered sensitive information. For example, if the individual is injured at an event promoted or delivered by the Organisation, health information may be collected about the individual in an emergency or otherwise with the individual's consent.

The Organisation may collect personal information about children (for example, when children participate in events the Organisation is involved with). Where children do not have sufficient maturity and understanding to make decisions about their personal information, the Organisation will require their parents or guardians to make decisions on their behalf.

Individuals can always decline to give the Organisation any personal information requested, but that may mean the Organisation cannot provide the individual with some or all of the services that are requested. If individuals have any concerns about personal information requested by the Organisation, please contact the Organisation.

<u>How and why does the Organisation collect and use individuals' personal information?</u>

Visitors to the Organisation's Websites
The way in which the Organisation handles the personal information of visitors to our websites is outlined below.

The Organisation collects personal information reasonably necessary to carry out the business, to assess and manage our participant's needs, and provide services to participants. The Organisation may also collect information to fulfil administrative functions associated with these services, for example billing, entering into contracts with individuals or third parties and managing participant relationships.

The purposes for which the Organisation usually collects and uses personal information depends on the nature of the individual's interaction with the Organisation, but may include:

- responding to requests for information and other general inquiries;
- Providing services to people;
- managing, planning, and administering programs, events, competitions and performances;
- researching, developing and expanding the Organisation's facilities and services;

- informing people of the Organisation's activities, events, facilities and services;
- recruitment processes (including for volunteers, internships and work experience); and
- responding to enquires and complaints;

The Organisation generally collects personal information directly from the individual involved. The Organisation may collect and update individuals' personal information over the phone, by email, over the internet, social media, or in person. The Organisation may also collect personal information about individuals from other sources. The Organisation may collect information from:

- affiliated and related companies; and
- third party suppliers and contractors who assist the Organisation to operate the business.

The Organisation also collects and uses personal information for market research purposes and to innovate the delivery of products and services.

How does the Organisation interact with individuals via the internet?
Individuals may visit the Organisation's websites (www.stgiles.org.au; www.arcss.com.au) without identifying their self. If individuals identify their self - for example, by providing their contact details in an enquiry, any personal information provided to the Organisation will be managed in accordance with this Privacy Policy.

The Organisation's websites may contain links to third-party websites. The Organisation is not responsible for the content or privacy practices of websites that are linked to the Organisation's website.

Can you deal with the Organisation anonymously?
The Organisation will provide individuals with the opportunity of remaining anonymous or using a pseudonym in their dealings with the Organisation where it is lawful and practicable - for example, when making a general enquiry. Generally, it is not practicable for the Organisation to deal with individuals anonymously or pseudonymously on an ongoing basis. If the Organisation does not collect personal information about the individual, the individual may be unable to utilise the Organisation's services or participate in events, programs or activities the Organisation manages or delivers.

How does the Organisation hold information?
The Organisation stores information in paper-based files or other electronic record keeping methods in secure databases (including trusted third party storage providers based in Australia and overseas). Personal information may be collected in paper-based documents and converted to electronic form for use or storage (with the original paper-based documents either archived or securely destroyed). The Organisation takes reasonable steps to protect individual's personal information from misuse, interference and loss and from unauthorised access, modification or disclosure.

The Organisation maintains physical security over paper and electronic data stores, such as through locks and security systems at the Organisation's premises. The Organisation also maintains computer and network security, for example, the use of firewalls (security measures for the internet) and other security systems such as user identifiers and passwords to control access to the Organisation's computer systems.

The Organisation's websites do not necessarily use encryption or other technologies to ensure the secure transmission of information via the internet. Users of the Organisation's websites are encouraged to exercise care in sending personal information via the internet.

The Organisation takes steps to destroy or de-identify information that is no longer required.

Does the Organisation use or disclose personal information for direct marketing?
The Organisation may use or disclose individuals' personal information for the purpose of informing the individual about the Organisation's services, upcoming promotions and events, or other opportunities that may interest the individual. Individuals who do not want to receive direct marketing communications, can opt-out at any time by contacting the Organisation. Individuals who opt-out of receiving marketing material

from the Organisation, may still be contacted by the Organisation in regard to its ongoing relationship with the individual.

How does the Organisation use and disclose personal information?

For participants

The purposes for which the Organisation may use and disclose participant personal information will depend on the services being provided to the participant. For example, if the participant has engaged the Organisation to deliver a service, the Organisation may disclose information about the participant to service providers where this is relevant to the Organisation's services.

Use and disclosure for administration and management

The Organisation will also use and disclose personal information for a range of administrative, management and operational purposes. This includes:

- administering billing and payments and debt recovery;
- planning, managing, monitoring and evaluating the Organisation's services;
- quality improvement activities;
- statistical analysis and reporting;
- training staff, contractors and other workers;
- risk management and management of legal liabilities and claims (for example, liaising with insurers and legal representatives);
- responding to enquiries and complaints regarding the Organisation's services;
- obtaining advice from consultants and other professional advisers; and
- responding to subpoenas and other legal orders and obligations.

Does the Organisation disclose your personal information overseas?

Other Uses and Disclosures

The Organisation may use and disclose individual's personal information for other purposes explained at the time of collection or otherwise as set out in this Privacy Policy.

Unless the Organisation has individuals' consent, or an exception under the Australian Privacy Principles applies, the Organisation will only disclose individuals' personal information to overseas recipients where the Organisation has taken reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to the individual's personal information.

How can individuals access or seek correction of their personal information?

Individuals are entitled to access their personal information held by the Organisation on request. To request access to personal information please contact the Organisation's Privacy Officer.

Individuals will not be charged for making a request to access their personal information but may be charged for the reasonable time and expense incurred in compiling information in response to the individual's request.

The Organisation will take reasonable steps to ensure that the personal information collected, used or disclosed is accurate, complete and up-to-date. Individuals can help the Organisation to do this by advising the Organisation if errors or discrepancies in information held about the individual is noticed, and also advising the Organisation if the individual's personal details change.

However, if an individual considers any personal information about them, which is held by the Organisation is inaccurate, out-of-date, incomplete, irrelevant or misleading, the individual is entitled to request correction of the information. After receiving a request from the individual, the Organisation will take reasonable steps to correct the information.

The Organisation may decline an individual's request to access or correct their personal information in certain circumstances in accordance with the Australian Privacy Principles. In circumstances where the Organisation refuses the individual's request, the Organisation will provide the individual with a reason for

the decision and, in the case of a request for correction, the Organisation will include a statement with the individual's personal information about the requested correction.

What should an individual do if they have a complaint about the handling of their personal information?
Individuals may contact the Organisation at any time if they have any questions or concerns about this Privacy Policy or about the way in which their personal information has been handled.

Individuals may make a complaint about privacy to the Privacy Officer. The Privacy Officer will first consider the individual's complaint to determine whether there are simple or immediate steps which can be taken to resolve the complaint. The Organisation will generally respond to the complaint within a week.

If the complaint requires more detailed consideration or investigation, the Organisation will acknowledge receipt of the complaint within a week and endeavour to complete the investigation into the complaint promptly. The Organisation may ask the complainant to provide further information about their complaint and the outcome they are seeking. The Organisation will then typically gather relevant facts, locate and review relevant documents and speak with individuals involved.

In most cases, the Organisation will investigate and respond to a complaint within 30 days of receipt of the complaint. If the matter is more complex or the investigation may take longer, the Organisation will let the complainant know.

If an individual is not satisfied with the Organisation's response to their complaint, or the individual considers that [*insert APP entity*] may have breached the Australian Privacy Principles or the Privacy Act, a complaint may be made to the Office of the Australian Information Commissioner. The Office of the Australian Information Commissioner can be contacted by telephone on 1300 363 992 or by using the contact details on the website *www.oaic.gov.au*.

Procedure
This section of the Privacy Policy and Procedure sets out the processes to be followed by the Organisation's staff in the event that the Organisation experiences a data breach or suspects that a data breach has occurred. A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, personal information.
The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (NDB Act) established a Notifiable Data Breaches (NDB) scheme requiring organisations covered by the Act to notify any individuals likely to be at risk of serious harm by a data breach. The Office of the Australian Information Commissioner (OAIC) must also be notified.

Accordingly, the Organisation needs to be prepared to act quickly in the event of a data breach (or suspected breach), and determine whether it is likely to result in serious harm and whether it constitutes an NDB.

This Procedure and Response Plan has been informed by:

- The Office of the Australian Information Commissioner's *"Guide to developing a data breach response plan*"
- The Office of the Australian Information Commissioner's *"Data breach notification guide: a guide to handling personal information security breaches*"
- NDB Act
- The Act and Australian Privacy Principles (Schedule 1 of the Act)

Process
Alert
Where a privacy data breach is known to have occurred (or is suspected) any member of the Organisation's staff who becomes aware of this must, within 24 hours, alert a Member of the Senior Leadership Team in the first instance.

The Information that should be provided (if known) at this point includes:

- When the breach occurred (time and date)
- Description of the breach (type of personal information involved)
- Cause of the breach (if known) otherwise how it was discovered
- Which system(s) if any are affected?
- Which directorate/faculty/institute is involved?
- Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach)
  A template can be found at Annexure A to assist in documenting the required information.

Assess and determine the potential impact
Once notified of the information above, the member of the Senior Leadership Team must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity.

Criteria for determining whether a Privacy Data Breach has occurred

- Is personal information involved?
- Is the personal information of a sensitive nature?
- Has there been unauthorised access to personal information, or unauthorised disclosure of personal information, or loss of personal information in circumstances where access to the information is likely to occur?

Criteria for determining severity

- The type and extent of personal information involved
- Whether multiple individuals have been affected
- Whether the information is protected by any security measures (password protection or encryption)
- The person or kinds of people who now have access
- Whether there is (or could there be) a real risk of serious harm to the affected individuals
- Whether there could be media or stakeholder attention as a result of the breach or suspect breach

Serious harm could include physical, physiological, emotional, economic/financial or harm to reputation and is defined in section 26WG of the NDB Act.

Having considered the matters outlined above, the member of the Senior Leadership Team must notify the Privacy Officer within 24 hours of being alerted under 3.1 of the *Australian Privacy Principles*.

Privacy Officer to issue pre-emptive instructions
On receipt of the communication by the relevant member of the Senior Leadership Team under 3.2 of the *Australian Privacy Principles*, the Privacy Officer will take a preliminary view as to whether the breach (or suspected breach) may constitute an NDB. Accordingly, the Privacy Officer will issue pre-emptive instructions as to whether the data breach should be managed at the local level or escalated to the Data Breach Response Team (Response Team). This will depend on the nature and severity of the breach. Where the Privacy Officer instructs that the data breach is to be managed at the local level, the relevant member of the Senior Leadership Team must:

- ensure that immediate corrective action is taken, if this has not already occurred (corrective action may include: retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system); and
- submit a report via the Privacy Officer within 48 hours of receiving instructions to do so. The report must contain the following:
  - Description of breach or suspected breach
  - Action taken
  - Outcome of action
  - Processes that have been implemented to prevent a repeat of the situation.
  - Recommendation that no further action is necessary

The Privacy Officer will be provided with a copy of the report and will sign-off that no further action is required.

Data breach managed by the Response Team

Where the Privacy Officer instructs that the data breach must be escalated to the Response team, the Privacy Officer will convene the Response Team and notify the Chief Executive Officer.

Primary Role of the Response Team

There is no single method of responding to a data breach and each incident must be dealt with on a case by case basis by assessing the circumstances and associated risks to inform the appropriate course of action.

The following steps may be undertaken by the Response Team (as appropriate):

- Immediately contain the breach (if this has not already occurred). Corrective action may include: retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.
- evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach having regard for the information outlined above
- Call upon the expertise of, or consult with, relevant staff in the particular circumstances.
- Engage an independent cyber security or forensic expert as appropriate.
- Assess whether serious harm is likely (section 26WG of the NDB Act).
- Make a recommendation to the Privacy Officer whether this breach constitutes an NDB for the purpose of mandatory reporting to the OAIC and the practicality of notifying affected individuals.
- Consider developing a communication or media strategy including the timing, content and method of any announcements to students, staff or the media.

The Response Team must undertake its assessment within 48 hours of being convened.

The Privacy Officer will provide periodic updates to the Chief Executive Officer as deemed appropriate.

Notification

Having regard to the Response Team's recommendation outlined above, the Privacy Officer will determine whether there are reasonable grounds to suspect that an NDB has occurred.

If there are reasonable grounds, the Privacy Officer must prepare a prescribed statement and provide a copy to the OAIC as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach).

The form can be located at https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB.

If practicable, the Organisation must also notify each individual to whom the relevant personal information relates. Where impracticable, the Organisation must take reasonable steps to publicise the statement (including publishing on the website).

The prescribed statement will be logged by the Privacy Officer.

Secondary Role of the Response Team

Once these matters have been dealt with, the Response Team should turn attention to the following:

- Identify lessons learnt and remedial action that can be taken to reduce the likelihood of recurrence, this may involve a review of policies, processes, refresher training
- Prepare a report for submission to the Chief Executive Officer.
- Consider the option of an audit to ensure necessary outcomes are effected and effective.

Relevant Legislation

- Privacy Act 1998
- Australian Privacy Amendment (Private Sector) Act 2000
- Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB Act)

Documents

- Confidentiality Policy and Procedure
- Code of Conduct
- Confidentiality Declaration