GOV-004 Privacy Policy

References:	Privacy Act 1988 (Cth) Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) Australian Privacy Principles Privacy and Data Protection Act 2014 (Vic) Public Records Act 1973 (Vic)
Associated Policies/Procedures:	ACA Constitution
Associated Forms:	

1. Introduction

From time-to-time the Australasian Corrosion Association ("the Association") is required to collect, hold, use and/or disclose Personal Information relating to individuals (including, but not limited to its members, contractors, suppliers, students and employees) in the performance of the Association's activities.

The information collected by the Association will, from time to time, be accessible to certain individuals employed or engaged by the Association who may be required to use the information in the course of their duties.

2. Purpose

This document sets out the Association's policy in relation to the protection of Personal Information, as defined, under the relevant Federal and State legislation. The obligations imposed on the Association under this policy are also imposed on any individual employed or engaged by the Association.

This policy outlines the Association's requirements and expectations in relation to the handling of Personal Information.

3. Scope

This policy applies to all employees, independent contractors, consultants and other persons engaged by the Association and who have access to Personal Information in the course of performing their duties.

4. Definitions

Term	Definition
APP	Australian Privacy Principles
Privacy Officer	The Privacy Officer is the first point of contact for advice on privacy matters in the Association
EO	The Executive Officer of the Association (sometimes referred to as the Chief Executive Officer or CEO)
Personal Information	Personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
Sensitive Information	Sensitive information includes, but is not limited to, information or an opinion about racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs, membership of a trade union, sexual preferences, criminal record, health information or genetic information.

5. Exempt information – employees

This policy does not apply to the collection, holding, use or disclosure of Personal Information that is an employee record as they are exempt from the Australian Privacy Principles (APP). An employee record is a record of Personal Information relating to the employment of an employee. Examples of Personal Information relating to the employment of the employee include, but are not limited to, health information and information about the engagement, training, disciplining, resignation, termination, terms and conditions of employment of the employee.

Employees (such as those engaged in a supervisory, operational or human resource capacity) will have access to employee records. Employees who have access to employee records must ensure that the information is handled confidentially and for a proper purpose only. Employee records are only permitted to be collected, used and disclosed where the act of doing so is directly related to a current or former employment relationship. Any records accrued or retained by the Association, whether employees, volunteers, clients, or any other sensitive body, are only to be used with the full consent of that person.

Employees who have access to employee records and who may have a question about the use or disclosure of employee records, should contact the Executive Officer for clarification.

6. Kinds of information that the Association collects and holds

The Association collects and holds Personal Information that:

a) is reasonably necessary for one or more of its functions; or

b) the Association has received consent to collect the information.

The Association must comply with both (a) and (b) above for Sensitive Information.

The information that the Association collects and holds for members will include among other things information collected by the means set out in item 7 below. However, the Association generally avoids holding birthdates of members.

The type of information that the Association collects and holds for non-members may depend on an

individual's relationship with the Association, for example:

6.1 **Candidate:** if a person is a candidate seeking employment with the Association, the Association may collect and hold information about that candidate including the candidates name, address, email address, contact telephone number, gender, age, employment history, references, resume, medical history, emergency contact, taxation details, qualifications and payment details.

6.2 **Customer:** if a person is a customer of the Association (such as a student enrolled in one of the Association's courses), the Association may collect and hold information, including the customer's name, address, email address, contact telephone number, gender and age and other Sensitive Information.

6.3 **Supplier:** if a person or business is a supplier of the Association, the Association may collect and hold information about the supplier including the supplier's name, address, email address, contact telephone number, business records, billing information and information about goods and services supplied by the supplier.

6.4 **Referee:** if a person is a referee of a candidate being considered for employment by the Association, the Association may collect and hold information including the referee's name, contact details, current employment information and professional opinion of the candidate.

The Association will only collect Sensitive Information where an individual consents to the collection of the information and the information is reasonably necessary for one or more of the Association's functions or activities.

Unsolicited personal information is Personal Information that the Association receives which it did not solicit. Unless the Association determines that it could have collected the Personal Information in line with the APPs or the information is contained within a Commonwealth record, it must destroy the information to ensure it is de-identified unless the Association determines that it is acceptable for the Association to have collected the Personal Information.

7. How the Association collects and holds Personal Information

The Association (and the employees acting on the Association's behalf) must collect Personal Information only by lawful and fair means. The Association may collect Personal Information in a number of ways, including without limitation:

- through application forms (e.g. job applications, Membership applications and renewals, student enrolments);
- by email or other communicative mechanisms;
- over a telephone call or video-conference call (including Teams, Zoom and Google Meetings);
- in person;
- through transactions;
- through the Association's and the C&P Conference's website;
- through lawful surveillance means such as a surveillance camera;
- by technology that is used to support communications between individuals and the Association, such as social media;
- through publicly available information sources (which may include telephone directories and the internet); and
- direct marketing database providers.

When the Association collects Personal Information about an individual through publicly available information sources, it will manage such information in accordance with the APPs.

At or before the time or, if it is not reasonably practicable, as soon as practicable after, the Association collects Personal Information, the Association must take such steps as are reasonable in the circumstances to either notify the individual or otherwise ensure that the individual is made aware of the following:

- the identity and contact details of the Association;
- that the Association has collected Personal Information from someone other than the individual or if the individual is unaware that such information has been collected;
- that collection of Personal Information is required by Australian law, if it is;
- the purpose for which the Association collects the Personal Information;
- the consequences if the Association does not collect some or all of the Personal Information;
- any other third party to which the Association may disclose the Personal Information collected by the Association;
- the Association's privacy policy contains information about how an individual may access and seek correction of Personal Information held by the Association and how an individual may complain about a breach of the APPs; and
- whether the Association is likely to disclose Personal Information to overseas recipients, and the countries in which those recipients are likely to be located.

8. Use and disclosure of Personal Information

The main purposes for which the Association may use and/or disclose Personal Information may include but are not limited to:

- recruitment functions;
- customer service management;
- training and events;
- surveys and general research; and
- business relationship management.

The Association may also collect, hold, use and/or disclose Personal Information if an individual consents or if required or authorised under law.

9. Direct marketing

The Association may use or disclose Personal Information (other than Sensitive Information) about an individual for the purpose of direct marketing (for example, advising a customer about new goods and/or services being offered by the Association).

The Association may use or disclose Sensitive Information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

An individual can opt out of receiving direct marketing communications from the Association by contacting the Privacy Officer in writing or if permissible accessing the Association's website and unsubscribing appropriately.

10. Disclosure of Personal Information

The Association may disclose Personal Information for any of the purposes for which it was collected, as indicated under clause 8 of this policy, or where it is under a legal duty to do so.

Disclosure will usually be internally and to related entities or to third parties such as contracted service suppliers.

If an employee discloses Personal Information to a third party in accordance with this policy, the employee must take steps as are reasonable in the circumstances to ensure that the third party does not breach the APPs in relation to the information.

The Association may be required to disclose Personal Information to overseas recipients. Before an employee on behalf of the Association discloses Personal Information about an individual to an overseas recipient, the employee will take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs in relation to the information.

The country or countries in which overseas recipients are likely to be located include the United States.

11. Access to Personal Information

If the Association holds Personal Information about an individual, the individual may request access to that information by putting the request in writing and sending it to the Executive Officer. The Association will respond to any request within a reasonable period, and a charge may apply for giving access to the Personal Information where the Association incurs any unreasonable costs in providing the Personal Information.

There are certain circumstances in which the Association may refuse to grant an individual access to Personal Information. In such situations the Association will provide the individual with written notice that sets out:

- the reasons for the refusal; and
- the method available to make a complaint.

If such a request is received, then the Privacy Officer should be contacted.

12. Correction of Personal Information

If the Association holds Personal Information that is inaccurate, out-of-date, incomplete, irrelevant or misleading, it must take steps as are reasonable to correct or delete the information.

If the Association holds Personal Information and an individual makes a request in writing addressed to the Privacy Officer to correct the information, the Association must take steps that are reasonable to correct the information and the Association will respond to any request within a reasonable period.

There are certain circumstances in which the Association may refuse to correct the Personal Information. In such situations the Association will give the individual written notice that sets out:

- the reasons for the refusal; and
- the mechanisms available to the individual to make a complaint.

If the Association corrects Personal Information that it has previously supplied to a third party and an individual requests the Association to notify the third party of the correction, the Association will take such steps as are reasonable to give that notification unless impracticable or unlawful to do so.

If such a request is received, then the Privacy Officer should be contacted.

13. Integrity and security of Personal Information

The Association will take such steps (if any) as are reasonable in the circumstances to ensure that the Personal Information that it collects is accurate, up-to-date and complete.

Employees must take steps as are reasonable in the circumstances to protect the Personal Information from misuse, interference, loss and from unauthorised access, modification or disclosure.

If the Association holds Personal Information and it no longer needs the information for any purpose for which the information may be used or disclosed and the information is not contained in any Commonwealth record and the Association is not required by law to retain the information, it will take such steps as are reasonable in the circumstances to destroy the information or to ensure it is de-identified.

14. Data Breaches and Notifiable Data Breaches

A Data Breach occurs where Personal Information held by the Association is accessed by, or is disclosed to, an unauthorised person, or is lost. An example of a Data Breach may include:

- Lost or stolen laptops or tablets;
- Lost or stolen mobile phone devices;
- Lost or stolen USB data storage devices;
- Lost or stolen paper records or documents containing Personal Information relating to the Employer's customers or employees;
- Employees mistakenly providing Personal Information to the wrong recipient (i.e. payroll details to wrong address);
- Unauthorised access to Personal Information by an employee;
- Employees providing confidential information to the Employer's competitors;
- Credit card information lost from insecure files or stolen from garbage bins;
- Where a database has been 'hacked' to illegally obtain Personal Information; and
- Any incident or suspected incident where there is a risk that Personal Information may be misused or obtained without authority.

If such an incident or event occurs, then the Executive Officer should be contacted.

Notifiable Data Breach occurs where there is an actual Data Breach, and:

- a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual (including harm to their physical or mental well-being, financial loss, or damage to their reputation); or
- in the case of loss (i.e. leaving an unsecure laptop containing Personal Information on a bus), unauthorised access or disclosure of Personal Information is likely to occur as a result of the Data Breach, and a reasonable person would conclude that the unauthorised access or disclosure would likely result in demonstrable harm to the relevant individual, inclusive of harm to their physical or mental well-being, financial loss, or damage to their reputation.

A Notifiable Data Breach does not include a Data Breach where the Association has been successful in preventing the likely risk of serious harm by taking remedial action.

If the Association is aware of any actual or suspected Data Breach, it will conduct a reasonable and expeditious assessment to determine if there are reasonable grounds to believe that the data breach is a Notifiable Data Breach or not.

Subject to any restriction under the Act, in the event that the Association is aware of a Notifiable Data Breach, the Association will, as soon as practicable, prepare a statement outlining details of the breach and notify:

- the individual whose Personal Information was part of the Data Breach; and
- the Office of the Australian Information Commissioner.

15. Anonymity and pseudonymity

Individuals have the option of not identifying themselves, or utilising a pseudonym, when anonymously dealing with the Association in relation to a particular matter. This does not apply:

- where the Association is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or
- where it is impracticable for the Association to deal with individuals who have not identified themselves or who have used a pseudonym.

However, in some cases, if an individual does not provide the Association with the Personal Information when requested, the Association may not be able to respond to the request or provide the individual/s with the goods or services that they are requesting.

16. Complaints

Individuals have a right to complain about the Association's handling of Personal Information if the individual believes the Association has breached the APPs.

Complaints will be dealt with in accordance with the Association's complaints procedure and the Association will provide a response within a reasonable period.

Individuals who are dissatisfied with the Association's response to a complaint, may refer the complaint to the Office of the Australian Information Commissioner.

17. Breach of this policy

An employee directed by the Association to do an act under this policy, and which relates to Personal Information, must ensure that in doing the act they comply with the obligations imposed on the Association. An employee directed by the Association who fails to do an act in accordance with this policy will be deemed to have breached this policy and will be subject to formal counselling and disciplinary action, up to and including possible termination of the employee's employment.

18. Accountabilities and responsibilities

18.1 **Board:** The ACA Board is ultimately responsible for approving and committing to the Privacy Policy.

18.2 **GovCom:** GovCom is responsible for reviewing this policy according to the policy review schedule and making recommendations to the Board for consideration as required.

18.3 **Executive Officer:** The Executive Officer is responsible for ensuring that appropriate resources, systems and processes are in place to implement the Privacy Policy across the Association; including the appointment of the Privacy Officer and the provision of training to staff.

18.4 **Privacy Officer:** The Privacy Officer is responsible for administering this policy as set out above.

19. Policy review

Nothing prevents the Governance Committee from amending this policy from time to time. Any amendments will be subject to Board approval. This policy is to be reviewed every three years.

This policy is to be available to Members on the Association's website.

Version	Change details	Reviewed by	Date reviewed	Approved by	Approval date
1.0	Policy development	GovCom	19 Oct 2017	Board	11 Nov 2017
1.1	Policy review	GovCom	20 Oct 2019	Board	11 Nov 2019
2.0	Update legislation and place in new template	GovCom	20 Sep 2024	Board	18 Sep 2024