Safety Institute of Australia

Trading as

Australian Institute of Health & Safety

effective from 1 July 2019

Privacy and Access

Operational administration and management of member and non-member personal information

Policy and Procedures

Policy active at: July 2019

Table of Contents

1. Background/ Purpose

As the Australian Institute of Health & Safety (AIHS) has grown and become more complex there is a need to ensure that we provide appropriate protection for the information we gather from members and non-members, ensuring good corporate governance and legal compliance with privacy legislation.

2. Protection of Privacy

Data that is collected from members by the AIHS belongs to the Safety Institute of Australia Inc (the National body). Therefore, access to the data must be controlled by the National body to ensure the AIHS discharges its legal obligations under relevant Privacy legislation.

In Australia, the privacy of information that is gathered by organisations is governed by the provisions of the *Privacy Act* (Cth) 1988 (the Act), which is binding on all entities, other than State Government entities. The Act outlines a set of Privacy Principles in a framework to which organisations must demonstrate compliance in order to discharge their legal obligations.

3. Privacy Principles

This policy is written in the context of national privacy principles outlined in Appendix #1 and are summarised below:

3.1 Collection of Data

- Collection of information must be necessary for the organisations function(s)
- Collection methods must be lawful and fair and not unreasonably intrusive.
- Information is currently collected when members join and through contact to update member information, usually by phone during business hours.
- When collecting information, the organisation must make known
    I. its identity
    II. inform the provider of the information that they can access the information

III. the purpose for collecting the information and who information may be disclosed to

IV. any law which requires particular information to be collected

V. the consequences of not providing information

3.2 Use and Disclosure

Information must not be disclosed for purposes other than that which it is collected for unless;

a. The reason for disclosure is related to the primary purpose of collection and the person would reasonably expect the information to be disclosed for this purpose.

b. The person has consented to its disclosure

c. Information is not sensitive information and is for the secondary purpose of direct marketing (subject to some restrictions – see Appendices 2 & 3)

d. Disclosure is required to protect public health or safety or to prevent illegal activity. (If disclosed for this purpose the disclosure and reason must be recorded)

e. Disclosure is required under law or by an enforcement body (subject to some restrictions – see Appendices 2 & 3) (If disclosed for this purpose the disclosure and reason must be recorded)

3.3 Data Quality

The organisation must take reasonable steps to keep information collected accurate, complete, and up to date.

3.4 Data Security

An organisation must take reasonable steps to protect personal information

3.5 Openness

There is a clear and open statement that sets out all the relevant Policies and Procedures regarding the collection, management, use, protection, and correction of the data that is gathered.

3.6 Access and Correction

The organisation must provide access to the individual on request (subject to any restrictions as outlined in this document)

3.7 Identifiers

The AIHS cannot use the same code or membership number as is used by another organisation and share that number for the purposes of identification as to do so would potentially breach that member's privacy.

3.8 Anonymity

This requires the AIHS to have an 'opt out' provision so that members do not necessarily have to identify themselves using their member identification. This is sometimes a requirement where a member may need to, for a variety of reasons, protect the knowledge of their location or contact details.

3.9 Transborder Data Flows

This requires an organisation to have procedures to manage transfers of information to a foreign country.

3.10 Sensitive Information

This requires an organisation to have procedures to manage collection of sensitive information e.g., health information.

4. AIHS Privacy Policy - Management of Personal Information

4.1 Statement

The Australian Institute of Health and Safety is committed to protecting the privacy of members and non-members and ensuring the security of personal information provided to the organisation. To this end we adopt the National Privacy Principles (Privacy Act 1988) The AIHS will apply best practice in the management of personal information whilst conducting our organisational activities.

Under the Privacy Act 1988 (Cth), personal information means information or an opinion, true or false and whether recorded in a material form or not, about an individual whose identity can be reasonably ascertained from that information or opinion.

This policy defines

- What personal information the AIHS collect
- How personal information is collected and maintained
- Who is information collected from?
- Why personal information is collected and how it is maintained and stored
- When and why information collected may be disclosed
- Access for members to their own information
- Security of Information
- A statement on the accuracy of information and
- A process for lodging a complaint in regard to information management.

4.2 What is collected:

1. Names
2. Address (personal and business)
3. Contact details including phone, e-mail, and other relevant details
4. Profile information

4.3 How information is collected and maintained:

1. We receive information from browsers when you visit our website, such as your server address, domain name, date and time of your visit, the pages visited and selected information for statistical purposes.
2. We receive information when you contact us in person or via the telephone, send us a facsimile or email or attend our functions or conferences.
3. We receive information on non-members from a wide range of personal contacts, referrals and from publicly available sources.

4. We receive information from you when you complete a range of forms associated with membership an, certification, and other matters.

4.4 Who is information collected from:

1. Members

2. Non-member enquiries

4.5 Why information is collected and how it is maintained and stored:

MEMBERS

1. The personal information is used to assess eligibility for membership of AIHS, record seminar/function and conference participation, conduct certifications, deliver communications, and validate member advancement.

2. Personal information is generally maintained and updated through the annual subscription process and by members updating their information using the AIHS webpage. We also may request personal information when you request information from us or apply to attend conferences or other AIHS sponsored events.

3. By ensuring that your profile information is current, you assist us to develop future strategies to benefit AIHS membership and to represent professional safety interests to government and industry more effectively and ensure that the AIHS is able to provide valuable services to you as a member.

4. Information is stored in written and/or electronic form

NON-MEMBERS

1. We collect and maintain personal information about non-members for the purpose of providing information to non-members about AIHS membership and services.

2. If you tell us, you do not wish us to provide you with information about membership or services, we will comply with your request.

4.6 When and why information may be disclosed:

1. We may disclose personal information that we collect about members or non-members to firms that perform services on our behalf in connection with maintaining

or servicing our membership or processing requests for products, services, or information, or in connection with market research purposes.

2. We may also disclose personal information if we are required or authorised to do so by law.

3. The AIHS does not make its member information available to direct marketing firms outside those directly engaged by the AIHS to perform functions directly relating to the purpose of the AIHS.

4.7 Access to member's personal information:

1. The information kept on members is available to that member through the members section of the website. Only staff at the national office of the AIHS and the individual member can access that information

2. Access to any member's personal information will only be given to that member upon verification of your identity.

3. If the AIHS denies you access to your personal information or refuses to make amendments to personal information we will provide you with reasons for doing so.

4.8 Confidentiality and Security:

All data is stored in written and/or electronic form and we maintain physical, electronic, and procedural safeguards to protect your personal information. We restrict access to personal information about members and non-members to those employees, corporate partners, joint venture partners and third-party providers who need to know that information to deliver our products and services efficiently and effectively. We are committed to ensuring that the personal information you provide remains confidential and secure.

4.9 Accuracy

We will take reasonable steps to ensure the personal information we maintain is accurate, complete, and up to date.

4.10 Complaints:

If you have a question, concern, or complaint regarding the way in which we handle your personal information, you should contact our Privacy Officer direct at:

Australian Institute of Health & Safety

PO Box 2078

GLADSTONE PARK VIC 3043

Or on 03 8336 1995

4.11 Changes to this policy:

From time to time it may be necessary for us to review this policy. We reserve the right to amend this policy at any time and to notify you of any amendments by posting an updated version on our website www.aihs.org.au.

Appendix #1 - Privacy Act Schedule 3 – National Privacy Principles

1 Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

(a) the identity of the organisation and how to contact it; and
(b) the fact that he or she is able to gain access to the information; and
(c) the purposes for which the information is collected; and
(d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and
(e) any law that requires the particular information to be collected; and
(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1 .3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2 Use and disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the **secondary purpose**) other than the primary purpose of collection unless:

(a) Both of the following apply:
  (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) The individual has consented to the use or disclosure; or

(c) If the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

(i) It is impracticable for the organisation to seek the individual's consent before that particular use; and

(ii) The organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(iii) The individual has not made a request to the organisation not to receive direct marketing communications; and

(iv) In each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(v) Each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; or

(d) If the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and

(iii) in the case of disclosure – the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or

(e) The organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health, or safety; or

(ii) a serious threat to public health or public safety; or

(f) The organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(g) The use or disclosure is required or authorised by or under law; or

(h) The organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

(i) The prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
(ii) The enforcement of laws relating to the confiscation of the proceeds of crime;
(iii) The protection of the public revenue;
(iv) The prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
(v) The preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully cooperating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:

(a) The individual:

(i) is physically or legally incapable of giving consent to the disclosure; or

(ii) physically cannot communicate consent to the disclosure; and

(b) A natural person (the carer) providing the health service for the organisation is satisfied that either:

(i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(c) The disclosure is not contrary to any wish:

(i) expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

(d) The disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is ***responsible*** for an individual if the person is:

(a) a parent of the individual; or
(b) a child or sibling of the individual and at least 18 years old; or
(c) a spouse or de facto spouse of the individual; or
(d) a relative of the individual, at least 18 years old and a member of the individual's household; or
(e) a guardian of the individual; or
(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or
(g) a person who has an intimate personal relationship with the individual; or
(h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

child of an individual includes an adopted child, a stepchild, and a foster child, of the individual.

parent of an individual includes a stepparent, adoptive parent, and a foster parent, of the individual.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew, or niece, of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, stepbrother, stepsister, foster-brother, and foster-sister, of the individual.

3 Data quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses, or discloses is accurate, complete, and up to date.

4 Data security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification, or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

5 Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses, and discloses that information.

6 Access and correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

(a) in the case of personal information other than health information – providing access would pose a serious and imminent threat to the life or health of any individual; or
(b) in the case of health information – providing access would pose a serious threat to the life or health of any individual; or
(c) providing access would have an unreasonable impact upon the privacy of other individuals; or
(d) the request for access is frivolous or vexatious; or
(e) the information relates to existing or anticipated legal proceedings between the

organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or

(f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(g) providing access would be unlawful; or

(h) denying access is required or authorised by or under law; or

(i) providing access would be likely to prejudice an investigation of

(j) possible unlawful activity; or

(k) providing access would be likely to prejudice:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of the public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders; by or on behalf of an enforcement body; or

(vi) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, those charges:

(a) Must not be excessive; and
(b) Must not apply to lodging a request for access.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete, and up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete, and up to date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete, and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete, or up to date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7 Identifiers

7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) an agency; or
(b) an agent of an agency acting in its capacity as agent; or
(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or
(b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or
(c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsection 100(2).

7.3 In this clause:

identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999)* is not an *identifier*.

8 Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9 Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

(a) The organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or

(b) The individual consents to the transfer; or

(c) The transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) All of the following apply:

(i) the transfer is for the benefit of the individual;
(ii) it is impracticable to obtain the consent of the individual to that transfer;
(iii) if it were practicable to obtain such consent, the individual would be likely to give it; or

(f) The organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used, or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

10 Sensitive information

10.1 An organisation must not collect sensitive information about an individual unless:

(a) the individual has consented; or
(b) the collection is required by law; or
(c) the collection is necessary to prevent or lessen a serious and Imminent threat to the life or health of any individual, where the individual whom the information concerns:
(i) is physically or legally incapable of giving consent to the collection; or
(ii) physically cannot communicate consent to the collection; or

(d) If the information is collected in the course of the activities of a non-profit organisation – the following conditions are satisfied:
(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;
(ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or

(e) The collection is necessary for the establishment, exercise, or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and
(b) the information is collected:
(i) as required by law (other than this Act); or
(ii) In accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) The collection is necessary for any of the following purposes:
(i) Research relevant to public health or public safety;
(ii) The compilation or analysis of statistics relevant to public health or public safety;
(iii) The management, funding or monitoring of a health service; and
(b) That purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(c) It is impracticable for the organisation to seek the individual's consent to the collection; and

(d) The information is collected:

(i) as required by law (other than this Act); or
(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or
(iii) In accordance with guidelines approved by the Commissioner under section 95A

for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:

non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.

Appendix #2 Internal guidelines for the use of AIHS Information

Access to Database Information

The AIHS National Office, under the direction of the CEO, is responsible for maintaining and managing the AIHS member database. This will involve the AIHS National Office responding to formal requests from members of the National Executive, State/Territory Branch networks and other AIHS committees (such as the College of Fellows or OHS Education Chapter) to format and distribute (within a specified timeframe) information to members nationally and internationally, or only to those AIHS members living within a particular Australian state or territory.

Such an approach will apply the *Permitted use of Database Information* outlined below and ensure that the most current member database information is used to distribute information to members. It will also enable the CEO / AIHS National Office to seek guidance and approval, if required, e.g., from the National Executive or relevant Division or Chapter Executive, prior to proposed information being distributed.

As the exception, any special requests from a Branch or other sub-group to the CEO for specific member information will need to be formally justified and be based on the minimum (read only) information required, e.g., member name and telephone number, as opposed to requesting all fields of the National or State / Territory member database information.

Permitted use of Database Information

This data can be used only in respect of the following activities:

- Contact with members from National or affiliated branches to confirm accuracy of the information in the database (address, telephone numbers, email addresses etc.);
- Contact with members from National or affiliated branches to follow up non-financial membership status;
- Contact with members from National or affiliated branches to advertise AIHS events.
- Contact with members from National or affiliated branches to advertise National elections and general meetings of the company
- Contact with members from National or affiliated branches to provide approved AIHS member services
- Contact with members from National or affiliated branches to request assistance with Divisional activities;

- Contact with new members from National or affiliated branches Affiliated Division to welcome them and arrange induction and/or introduction to Division;
- Contact with members from National or affiliated branches or committees to offer assistance and mentoring

Prohibited Use of the Database

The database and the information contained in it can only be used for AIHS business and activities and cannot be used for any of the following:

- For personal or reputational gain of the individual who has been given access to the database
- For distribution of information (personal or otherwise) on behalf of a candidate for election or self-promotional purposes
- To create another database or distribution list for the purposes of sending broadcast email or posting out mailing pieces
- Be given to or access given to any third party (including any individual member of the AIHS) for the purposes of allowing them to promote themselves or any product or service that they may be associated with
- For any reason not approved by the AIHS National Board of Management.

Database Management

The database and its contents are in the custody of and will be exclusively managed on behalf of the AIHS by the National Office.

Where member information is identified as incorrect the database may be corrected either by;

1. The individual member can go into the members area and update their own personal details; or
2. The Division sends some advice to the National Office requesting that the information be updated; or
3. The national office becomes aware of changes in members personal information and subsequently updates that information.

Email Broadcasts and Mail outs

- Email distribution to full list done by National Office within 2 working days of request (request approved by CEO)
- Email distribution to selected list (i.e., whole of Branch) within 3 working days of request (request approved by CEO)
- Email distribution to small groups (selected membership within National membership or within branches) within 3 working days (approved by CEO on confirmation with National Executive) [specially created distribution list to be deleted upon completion]
- National Mail out sent to mailing house within 2 days of mailing piece being finalised and printed.
- National Mail out printed within one week of artwork being approved and finalised.
- Branch Mail out (mailing list to be provided to mailing house or distribution organiser) within 3 working days of request on proviso that use is one off and mailing list is destroyed/deleted upon completion of mailing/distribution.

Appendix 3 – Use of AIHS Website and Discussion Forums

Website Privacy Statement

1. Personal information collected when you use our website

The Privacy Act (Cth) 1988 defines Personal Information to be "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."

When you visit this website, we may collect different kinds of Personal Information from you in a variety of ways.

(a) Clickstream Data

When you visit this website, our server makes a record of your visit and logs the following Personal Information:

- Your server address;
- Your top-level domain name (for example .com, .gov, .au, .net, .edu, etc);
- The time and date of your visit to the website;
- The pages and documents you have accessed or viewed; and
- The type of browser you are using.

(b) Emails and Electronic Forms

The Personal Information collected by AIHS when you send us an email, or if you complete and submit one of the electronic forms on our website, will include your email address and may also include some of your Personal Information. Personal Information will only be used for the stated purpose for which it was provided.

AIHS records your email address and Personal Information in the following instances:

- When you subscribe to and receive the online newsletters
- When you send feedback via email or electronic forms.

This Personal Information will not be disclosed to a third party, other than our development team for the purposes of testing, validating, or upgrading online AIHS services, without your express consent.

(c) Our use of cookies

A cookie is a small amount of information stored on your computer by the AIHS website server. It is information that your web browser sends back to the AIHS website server whenever you visit it again. Cookies are used to 'remember' your browser between page visits. In this situation, the cookie identifies your browser, not you personally. No Personal Information is stored within the AIHS cookies.

Purpose and use of Personal Information we collect from you

The Personal Information we collect from you is collected for the following purposes:

- Website and system administration, including monitoring to prevent security breaches;
- Enhancement to the website to the user's needs; and
- Communication, statistics, research, and development.

No attempt will be made to identify individual users or their browsing activities other than as disclosed in this privacy statement or as required by law.

The Personal Information collected on this website will not be disclosed to a third party except where authorised by you or required by law.

2. Publication of your Personal Information

We will only publish Personal Information on this website if it has been collected for this purpose with your knowledge, or if you have otherwise consented to the disclosure.

When giving such consent you should be aware that Personal Information published on this website is accessible to millions of users from all over the world, that it will be indexed by search engines and that it may be copied and used by any web user. This means that, once the Personal Information is published on this website, we will have no control over its subsequent use and disclosure. For example, participation in any of the open forum services mentioned above may involve submitting your email address and Personal Information into the public domain.

All Personal Information collected by the AIHS is protected by the Privacy Act (Cth) 1988 and any subsequent Federal legislation. Information on the Commonwealth Privacy Act 1988 can be found on the Federal Privacy Commissioner's website http://www.privacy.gov.au/.

3. Access to the Personal Information we collect

If you wish to know what, if any, Personal Information we hold about you, or wish to correct any Personal Information we may hold about you, you may access and correct such Personal Information at any time by contacting us using the contact information provided.

4. Security of your Personal Information

Your Personal Information will be held in strictest confidence. We take all reasonable steps to ensure that the Personal Information we hold in our servers is not subject to loss, misuse or unauthorised access or alteration. We also take reasonable steps to destroy or permanently de-identify Personal Information if it is no longer required.

This website does not, however, provide facilities for the secure transmission of information across the Internet. You should be aware that there are inherent risks associated with the transmission of Personal Information via the Internet.

You should also note that if you link to a non-AIHS website from this website, a different privacy and security statement is likely to apply. Therefore, once you leave this website, you should check the online privacy and security statements of the new website you are visiting.