

IPSHA Privacy Policy

Current version:	October 2024
Last reviewed:	
Next review date:	October 2026
Person responsible for review:	Executive Officer

IPSHA Privacy Policy

IPSHA Limited ABN 31 059 221 877 (IPSHA) is strongly committed to protecting your privacy. Any personal information you provide us (or which we otherwise collect about you) will only be used, collected and disclosed in accordance with this policy.

The Australian Privacy Principles

IPSHA has adopted effective privacy practices under the Privacy Act and APPs where applicable.

The Privacy Act 1988 (Privacy Act) and the Australian Privacy Principles (APPs) apply to Australian Government agencies, organisations with an annual turnover of more than \$3 million, and some other organisations with annual turnovers of less than \$3 million. The Privacy Act and the APPs do not currently apply to IPSHA.

The kinds of Information we collect and hold

In relation to members, we collect a range of personal information about you, for example:

- (a) your name, email address, work phone number, that will be published on the IPSHA website Member Directory, visible to all IPSHA members through password access.
- (b) to help us understand the diversity within IPSHA members and schools for planning only purposes, we ask for voluntary sensitive information on: gender, languages other than English, Religion, identification as Aboriginal and Torres Strait Islander, education sectors you have worked in, the year you commenced as a Head, year born and highest level of qualification. This information will not be published on the IPSHA website Member Directory and held securely in the IPSHA Member Management System.
- (c) information about your school, your role and responsibilities, and your experiences;
- (d) information about your health and dietary needs, to the extent that this information may be relevant to IPSHA's ability to safely operate events or activities, or IPSHA's (and its service provider's) ability to safely provide services to you;
- (f) your photograph provided and at IPSHA events to publish them to other members or on the website and social media;
- (g) photographs and videos of you taken at IPSHA events or activities.
- (h) banking or credit card details through our online merchant if you want to make payments electronically (eg conference or special event fees).
- (i) personal information regarding directors as required by the Corporations Act 2001.
- (j) personal information regarding prospective employees to assess their suitability for potential employment with us.

(k) personal information from other stakeholders (including sponsors, those who attend IPSHA activities or events, service providers, and those we otherwise communicate with) for the purpose of performing activities and operations in furtherance of IPSHA's purpose.

(l) IPSHA will not pass on personal contact details to IPSHA sponsors without the written consent of the member.

How we collect personal information

Information (including personal information about you) is obtained from you at the beginning of your membership, when we communicate with or about you, or at any other time you update your details.

Use and disclosure of information collected

IPSHA will only use and disclose your information for the purpose of communicating with you (including direct marketing), conducting internal research, analysis and statistics, performing activities or operations in furtherance of its purpose, or otherwise enabling you to enjoy the benefits and services afforded by IPSHA membership.

You may request not to receive direct marketing/communications materials from us.

Please use the member enquiry or contact us if you wish to change your communication preferences.

Our website allows members to find other members' names and email addresses, through the IPSHA Members Directory. These details are also provided to other Branch Members for the purpose of supporting collegiality and sharing of professional knowledge.

In the course of our activities, we may disclose your personal information to our conference organisers, contractors, consultants, banks, accountants, lawyers, insurers or advisors. This is done only when considered appropriate to better provide you with access to relevant benefits and services and on a need-to-know basis. We take steps to ensure that those persons keep that information secure and confidential and delete the information when it is no longer needed, where possible.

Our technology suppliers use of cloud infrastructure or servers **is located in Australia**.

Accessing and correcting your personal information

It is important to us that the information we hold about you is accurate. You may request access to your personal information and ask us to correct it if you think it is incorrect.

We will take reasonable steps to update or correct, as soon as possible, any information in our possession that is inaccurate, incomplete, out-of-date, irrelevant or misleading.

You may ask us to delete personal information and, to the extent that we are able to, we will delete that information.

We may refuse to grant you access to your personal data where this is allowed or required by law. If we do refuse to grant access, we will give you written reasons.

If you would like to access your personal information, please contact: National Executive Officer:
executiveofficer@ipsha.org.au

Internet Security

Notably parts of the IPSHA website may not provide facilities for the secure transmission of information across the Internet. Users should be aware that there are inherent risks when transmitting information across the Internet.

Data security

We strive to ensure the security of personal information we collect and hold and take data protection seriously. We take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification and disclosure.

We also regularly review and update our physical and data security measures in light of current technologies and the requirements of applicable laws.

To ensure member data is secure, an IPSHA Member Management System has been created with Two factor authentication set up for approved user access.

Unauthorised Access

Under the Notifiable Data Breach (NDB) scheme, IPSHA will notify affected individuals and the Office of the Australian Information Commissioner (OAIC) about an eligible data breach where required to do so by law.

An eligible data breach occurs when:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that IPSHA holds.
- this is likely to result in serious harm to one or more individuals, and
- IPSHA has not been able to prevent the likely risk of serious harm with remedial action.

Contacting Us

Should you have a concern or question on IPSHA's privacy policy, please feel free to contact us at: executiveofficer@ipsha.org.au.

If you have a complaint about our handling of your personal information, you should address your complaint in email to the IPSHA Executive Officer at: executiveofficer@ipsha.org.au