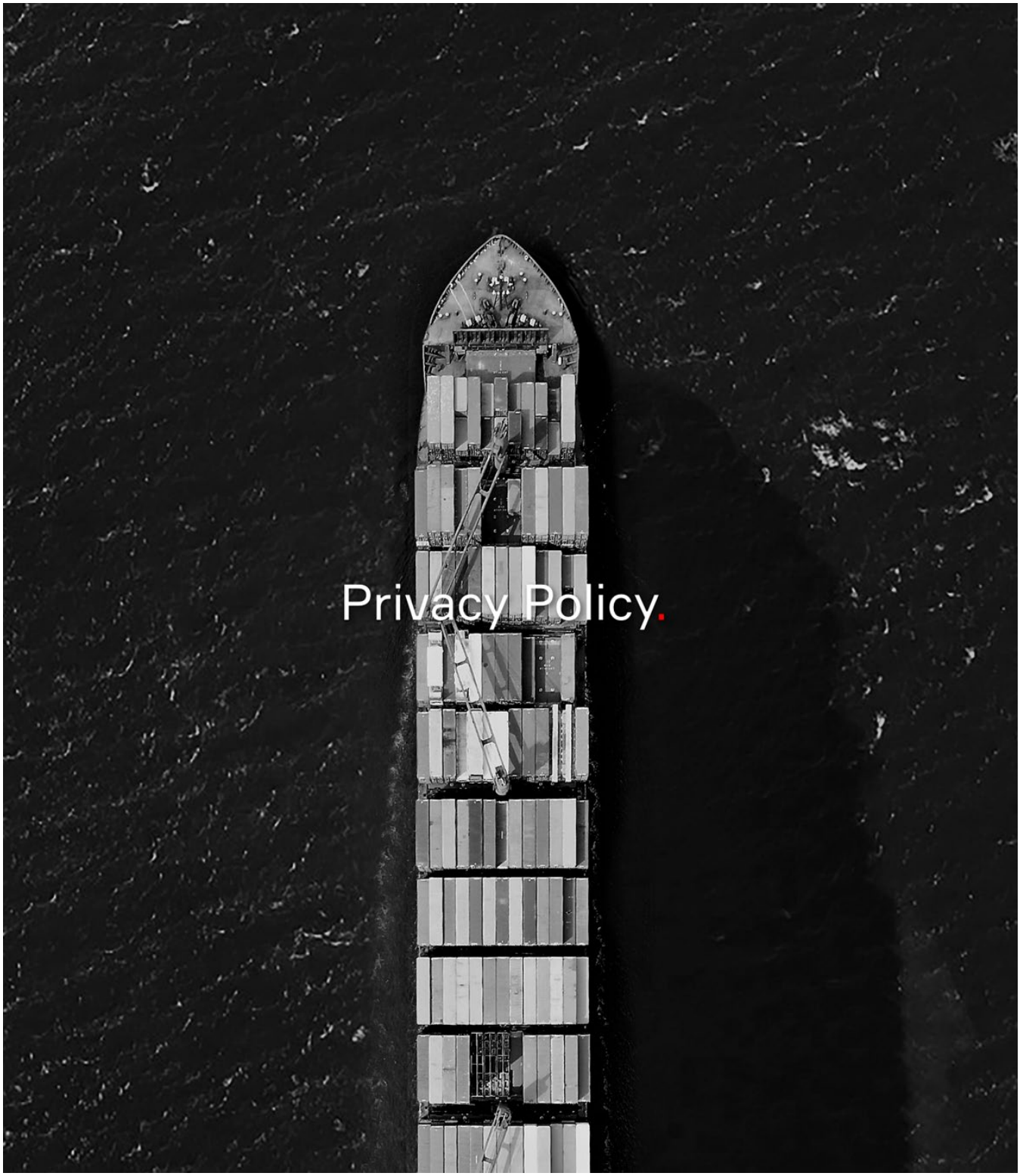
AWH

Realise the Possibilities.

Effective Date:	10 December 2020
Approved by:	CEO
Custodian:	General Counsel
Next Review:	December 2021
Document Number:	13
Version Number:	5



1. OVERVIEW OF THIS POLICY

This Policy details how we comply with the Privacy Act, including the Australian Privacy Principles, which have been introduced under the Privacy Act.

This Policy does not apply to the collection or use of information about corporations.

If you would like a hardcopy of this Policy, please contact the Privacy Officer on (03) 5272 9200.

2. DEFINITIONS

2.1. **APPs** means the Australian Privacy Principles introduced under the Privacy Act;

2.2. **Information** is used in this Policy to describe Personal Information and Sensitive Information;

2.3. **Personal Information** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

2.3.1. whether the information or opinion is true or not; and

2.3.2. whether the information or opinion is recorded in a material form or not;

2.4. **Policy** means this Privacy Policy;

2.5. **Privacy Act** means the Privacy Act 1988 (Cth) as amended from time to time;

2.6. **Sensitive Information** is defined in the Privacy Act to include information or opinions about an individual's racial or ethnic origin; political opinions or associations; religious or philosophical beliefs; trade union membership or associations; sexual orientation or practices; criminal record; health or genetic information; some aspects of biometric information;

2.7. **We**, **Us**, and **Our** refer to AWH Pty Ltd (ACN 069 066 842) (ABN 81 069 066 842).

3. THE TYPE OF INFORMATION WE COLLECT

3.1. Personal Information

Personal information that we collect and hold is information that is reasonably necessary for the proper performance of our functions and activities as a supplier of services.

While the type of Personal Information we collect and hold may vary, generally it will include the following:

3.1.1. general identification information, such as your name, date of birth, gender, job title and occupation;

3.1.2. contact details, such as address, telephone numbers and email address and Internet Protocol (IP) address;

3.1.3. usernames and passwords;

3.1.4. educational qualifications, employment history and referee reports;

3.1.5. information contained in identification documents, such as passport or driver's licence;

3.1.6. Government issued identification numbers, such as tax file numbers;

3.1.7. financial information, such as credit card and bank account details, including details relating to credit history, transaction history, credit capacity, and eligibility for credit;

3.1.8. details of superannuation and insurance arrangements;

3.1.9. visa or work permit status and related information;

3.1.10. association membership details;

3.1.11. personal references;

3.2. Sensitive Information

We may at times, subject to this Policy, also collect and hold Sensitive Information.

4. COLLECTION

We collect Information only by fair and lawful means where it is reasonable and practicable to do so. We do so in order to conduct our business, to provide and market our services and to meet our legal obligations.

If you do not provide us with Information we reasonably request, we may not be able to provide the requested services to you. We also may not be able to provide you with the information about the services that you may want.

4.1. How we Collect Information

4.1.1. Generally, we collect Information that from you directly when you:

4.1.1.1. visit our website (www.awh.com.au);

4.1.1.2. attend events we organise, such as auctions;

4.1.1.3. submit an application or resume with us;

4.1.1.4. speak to us on the telephone or in person; and

4.1.1.5. write to us (including email correspondence).

4.1.2. Sometimes we collect Information from outside sources, such as marketing mailing lists and other public information (including public posts to social networking sites such as LinkedIn and Twitter) and commercially available personal, identity, geographic and demographic information.

4.1.3. We may also collect Information from other people when it is necessary for a specific purpose, such as checking information that you have given us or where you have consented, or would reasonably expect us, to collect your Information in this way.

If it is unclear to us whether you have consented to the collection of Information from a third party, we will take reasonable steps to contact you to ensure that you are aware of the reason and purpose of the collection.

If we collect Information from a third party, we will inform you that the Information has been collected and the circumstances of such collection.

4.1.4. We will also collect Information about you if we are required to do so under an Australian law. If so, we will inform you of this, including details of the law requiring the collection.

4.1.5. We may also collect Information about you from a range of publicly available sources including newspapers, journals, directories, the internet and social media sites.

4.2. Specific Technology Issues

It is important that you understand that there are risks associated with use of the internet and you should take all appropriate steps to protect your Information. You can contact us by land line telephone or post if you have concerns about making contact via the internet.

We may use cookies when you visit our website (www.awh.com.au) and, as a consequence, we may collect certain information from you such as:

4.2.1. your browser type;

4.2.2. your location;

4.2.3. your IP address;

4.2.4. information about when and how you use our website; and

4.2.5. information about your past internet usage, such as websites you visit before coming to our website and documents you have downloaded.

Our website may contain links to other sites. We are not responsible for the privacy practices or the content of any sites linked to our website.

4.3. Unsolicited Information

Where we receive unsolicited Information about you, we will check whether that Information is reasonably necessary for our functions or activities. If it is, we will handle that Information in the same way we do other Information we seek from you. If not, we will destroy or de-identify it.

5. REASON FOR COLLECTION & USE

5.1. Personal Information

We will only use your Information if we have a lawful reason to do so, such as when it is our legal duty, if we have your consent and when it is in our legitimate interest to do so.

We will only use and disclose your Personal Information for the primary purpose for which it is collected, for reasonably expected secondary purposes which are related to the primary purpose and in other circumstances authorised by the Privacy Act. In general, we use and disclose your Personal Information to:

5.1.1. conduct our business;

5.1.2. provide and market services;

5.1.3. communicate with you and assist you with enquiries;

5.1.4. purchase from you;

5.1.5. comply with our legal obligations, including Work Health & Safety; compliance; governance and Chain of Responsibility obligations;

5.1.6. help us manage and enhance our services;

5.1.7. gain an understanding of your needs;

5.1.8. establish an account for you;

5.1.9. carryout other administrative tasks, such as, processing payment transactions, charging and billing, detecting or preventing fraud, identifying breaches of our terms and conditions;

5.1.10. give you access to specific sections of our website; and

5.1.11. improve your online experience with us.

5.2. Sensitive Information

We will not collect Sensitive Information about you unless:

5.2.1. we obtain your explicit consent to collect and use such Sensitive Information, or:

5.2.2. the Sensitive Information is reasonably necessary for one or more of our functions or activities; or

5.2.3. the collection of the Sensitive Information is required or authorised by or under Australian law or a court/tribunal order; or

5.2.4. a permitted general situation exists in relation to the collection of the Sensitive Information by us; or

5.2.5. a permitted health situation exists in relation to the collection of the Sensitive Information by us.

6. DISCLOSURE

6.1. Disclosure of Personal Information

Where necessary for our business we may disclose Personal Information to other non AWH organisations in Australia, such as:

6.1.1. our service providers;

6.1.2. financial institutions;

6.1.3. credit providers, credit reporting bodies;

6.1.4. insurers; and

6.1.5. nominated referees.

6.2. **Disclosure to Related Entities**

We may disclose Information to our related entities.

7. MARKETING

We may use and/or disclose your Information in order to:

7.1. provide you with news and information about our services;

7.2. provide you with marketing and promotional material that we believe you may be interested in; or

7.3. seek your feedback on our services.

We do not disclose your Information to third parties for the purpose of allowing them to send marketing material to you.

Only with your express consent will we use or disclose Information about you for the purposes of direct marketing. You can ask us not to do this at any time by writing to The Privacy Officer, AWH Pty Ltd, PO Box 283, Lara, Victoria, 3212.

We will not sell your Information.

8. SECURITY & MANAGEMENT

We take reasonable steps to protect your Information against misuse, interference, loss, unauthorised access, modification and disclosure. The protective steps we take include:

8.1. confidentiality requirements of our employees;

8.2. document storage security policies;

8.3. security measures for restricted access to our systems;

8.4. deletion, destruction or de-identification of Information where it is no longer required by us; and

8.5. the maintenance of a Notifiable Data Breaches – Policy & Response Plan (Annexure 1).

9. CORRECTION

We aim to ensure that the Information we hold is accurate, complete and up-to-date. We encourage you to contact us in order to update any Information we hold about you. Our contact details are set out at the end of this Policy.

If you contact us regarding an apparent inaccuracy in relation to your Information and we are satisfied that the Information is inaccurate, out-of-date, incomplete, irrelevant or misleading, then reasonable steps will be taken to correct the Information within 30 days, or a longer period as we agree with you in writing.

We will not charge you for a correction.

If we determine that the correction is not required, we will provide you with written notice stating the reasons why the correction was not made and refer you to our complaints procedure.

If a correction is made to any Information that was previously disclosed to a third party, as long as it is reasonable to do so, we will give each such recipient written notice of the correction within a reasonable period. We will also notify you that the correction has been made.

10. ACCESS TO YOUR INFORMATION

You are entitled to access your Information held by us.

If you wish to access your Information, you must lodge a request for access by contacting the Privacy Officer, by post at AWH Pty Ltd, PO Box 283, Lara, Victoria, 3212; or by email on jda@awh.com.au.

We may charge a fee to cover our reasonable costs in meeting an access request. You will be provided with access to your Information within 30 days of the request (unless unusual circumstances apply).

We are not required to give you access to your Information if:

10.1. it would be unlawful to do so; or

10.2. denying access is required or authorised by Australian law or a court/tribunal order; or

10.3. to do so would likely prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

If we do not give you access to your Information you will receive written notice that explains the reason for the refusal.

11. COMPLAINTS

Complaints about alleged breaches by us of the Privacy Act, the APPs or this Policy can be made by contacting the Privacy Officer by post at AWH Pty Ltd, PO Box 283, Lara, Victoria, 3212; or by email on jda@awh.com.au. If you do not consider that your complaint has been adequately dealt with by us, you may make a further complaint to the Office of the Australian Information Commissioner, which has complaint handling responsibilities under the Privacy Act.

12. ACCESS TO THIS POLICY

This Policy will be reviewed from time to time to take account of new laws and technology, changes to our operations and practices and the changing business environment.

The most current version of this Policy will be uploaded to our website (www.awh.com.au) or can be obtained by contacting our Privacy Officer:

E-Mail: jda@awh.com.au

Phone: (03) 5272 9200

Postal Address: PO Box 283, Lara, Victoria, 3212

13. FURTHER INFORMATION

If you have any questions about privacy-related issues, please contact our Privacy Officer.

For further information about privacy, the protection of privacy and credit reporting can also be found on visit the Office of the Australian Information Commissioner's website at www.oaic.gov.au

AWH
Australia's Largest Warehouse Provider.

Annexure 1:
Notifiable Data Breaches – Policy & Response Plan

1. **PURPOSE**

The purpose of this annexure to the Privacy Policy is to ensure there are clear procedures in place for the management and notification of data breaches in order to comply with the Privacy Amendment (Notifiable Data Breaches) Act 2017 (an amendment to the Privacy Act 1988) effective 22 February 2018.

2. **POLICY STATEMENT**

We are committed to ensuring an environment with clear procedures and processes for privacy data breaches. We have obligations under the Privacy Act to put in place reasonable security safeguards and to take active steps to protect the personal information that it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.

3. **SCOPE**

This policy applies to, but is not limited to all:

3.1. our employees, agents, directors and officers; and

3.2. third party suppliers and contractors who provide services to us.

4. **NOTIFIABLE DATA BREACHES**

We are required to comply with the Privacy Act.

The Notifiable Data Breach scheme obliges all organisations required to comply with the Privacy Act to notify any individuals likely to be at risk of serious harm by a data breach.

4.1. **What is a notifiable data breach?**

A Notifiable Data Breach is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates.

A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure. Examples of a data breach include when:

4.1.1. a device containing customers' personal information is lost or stolen

4.1.2. a database containing personal information is hacked

4.1.3. personal information is mistakenly provided to the wrong person.

13.1. **What is "Serious Harm"?**

"Serious Harm" is not defined in the Privacy Act.

In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial or reputational harm.

Whether a data breach is "likely to result" in serious harm to an individual whose information was part of the data breach requires an objective assessment from the perspective of a reasonable person. Under this scheme a "reasonable person" means a person in the entity's position (rather than the position of an individual whose personal information was part of the data breach or any other person), who is properly informed, based on information immediately available and/or following reasonable inquiries or an assessment of the data breach.

The phrase "likely to result" means the risk of serious harm to an individual is more probable than not.

In assessing whether a data breach is "likely to result" in serious harm the following needs to be considered:

the type or types of personal information involved in the data breach;

the circumstances of the data breach; and

the nature of the harm that may result from the data breach.

Assessing the degree of harm caused as a result of a data breach – and whether the data breach is notifiable – will be undertaken by the Data Breach Response Team.

5. **RESPONSE TO DATA BREACHES**

We have a robust approach to protection of personal information, and this is reflected in our Incident Response Plan at Attachment 1 and Incident Reporting Plan at Attachment 2.

We are committed to following this policy and the Incident Response Plan for a number of reasons including:

5.1. mandatory compliance with the Privacy Act;

5.2. maintaining the protection of the personal information of all stakeholders; and

5.3. instilling confidence in our capacity to protect personal information as well as responding appropriately to a data breach.

6. DATA BREACH RESPONSE TEAM

The Data Breach Response Team is comprised of the individuals across We who are best placed to determine the response to a potential data breach. The Data Breach Response Team will be coordinated by General Counsel but at a minimum, the team includes:

6.1. General Counsel

6.2. Chief Information Officer

6.3. General Manager (of the sector within our organisation with the relevant breach).

7. ROLES AND RESPONSIBILITIES

This section outlines the responsibilities of management and staff in relation to notifiable data breaches. (Refer to Attachments 1 and 2)

Role	Responsibility
All Staff	Escalate a data breach, or suspected data breach, to their Manager (or General Counsel if their Manager is unavailable) as soon as it becomes known
Manager	Escalate the data breach, or suspected data breach, to General Counsel and the CIO
CIO	Contain (if possible) the breach and prevent additional information loss; start forensic examination into the source, and extent, of the breach; implement measures to prevent a further data breach; liaise with third party I.T. providers as required
General Counsel	Assess the extent and cause of the breach and any potential serious harm to any individual(s); brief the CEO; determine which individuals and (possible) organisations (including insurers) are required to, or should, be notified; consider any legal or contractual obligations that may arise
Data Breach Response Team	Assess and contain the breach as soon as possible; notify the individual(s) affected if required; notify any relevant organisations if appropriate; notify the Office of the Information Commissioner if required
CEO	Ensure We have an appropriate policy and response plan in place to comply with the Privacy Act

8. DEFINITIONS

8.1. **APPs** means the Australian Privacy Principles introduced under the Privacy Act;

8.2. **Notifiable Data Breach** means a data breach that is likely to result in serious harm to any of the individuals to whom the information relates. It occurs when personal information held by us are lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.

8.3. **OAIC** means the Office of the Australian Information Commissioner

8.4. **Personal Information** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

8.4.1. whether the information or opinion is true or not;

8.4.2. whether the information or opinion is recorded in a material form or not; and

8.5. **Privacy Act** means the Privacy Act 1988 (Cth) as amended from time to time.

9. INTERACTING POLICIES AND LEGISLATION

This policy should be read in conjunction with the Privacy Act 1988 (Cth)

Attachment 1: Incident Response Plan

Maintain personal information security (APP 11)

APP entities must take reasonable steps to protect personal information they hold.

Possible data breach occurs

Contain

As your first priority, take immediate steps to contain the possible data breach.

Assess

Consider whether the breach is likely to result in serious harm for any of the individuals whose information is involved.

If you have reasonable grounds to believe there is an eligible breach, you must notify. If you only have reasonable grounds to suspect an eligible breach, you must conduct a reasonable and expeditious assessment of whether there is a notifiable breach, usually within 30 days (26WH).

Take remedial action

Where possible, an entity should take steps to reduce the likelihood of harm to affected individuals caused by the breach. This might involve recovering the information, or providing assistance to affected individuals.

If remedial action is able to make serious harm not likely, then notification is not required, and entities can proceed directly to 'Review' (26WF).

Notify

Where serious harm to affected individuals is likely, the entity must notify those individuals and the Commissioner (26WK; 26WL). The notification must contain the entity's contact details, a description of the breach, the kind/s of information concerned, and recommended steps for individuals. It may contain other information.

If practicable, notify those individuals at likely risk of serious harm directly. If it is not practicable to notify directly, you can publish a statement on your website, and take steps to draw it to the attention of the relevant individuals.

In certain circumstances, an exception may apply meaning notification is not required (26WM – 26WQ)

Review

Consider how the breach occurred and whether to enhance your personal information security measures.

Attachment 2: Incident Reporting Plan