ACCEPTABLE USE OF ARTIFICIAL INTELLIGENCE POLICY

ARA Group Limited ABN 47 074 886 561 and its related corporate entities (collectively **ARA Group**) are committed to managing operational risks and maintaining confidentiality, including maintaining appropriate measures to ensure artificial intelligence is used appropriately.

1 Purpose

This Acceptable Use of Artificial Information Policy (**Policy**) forms part of ARA Group's risk management and governance resources and serves to:

(a) outline the acceptable use and guidelines for the use of an artificial intelligence language model (**AILM**), such as ChatGPT, Zapier or other similar tools, by employees, contractors or other third parties;

(b) protect ARA Group and its directors, officers, employees and personnel (together **Employees**) from exposure to risks such as the compromise of network systems and services, compromise of confidential information, loss of intellectual property, and legal liability;

(c) ensure that the use of artificial intelligence is ethical, lawful, and in compliance with all applicable laws, regulations and ARA Group policies; and

(d) put Employees on notice that certain IT Facilities may be subject to surveillance by ARA Group to ensure compliance with this Policy.

2 Application

2.1 This Policy applies to all Employees of ARA Group and any other parties acting as representatives or agents of ARA Group, irrespective of whether employment is conducted within ARA Group's office locations, on various worksites, from home or otherwise.

2.2 This Policy governs conduct in connection with employment with ARA Group and all conduct generally involving the use of AILM which may adversely affect ARA Group or ARA Group's confidence and trust in its Employees.

2.3 This Policy applies whether access to AILM is being used in connection with an Employee's employment through company-owned or Employee owned equipment.

3 Privacy

Privacy considerations only apply to this Policy with respect to matters covered by the *Privacy Act 1988* (Cth), ARA Group's Privacy Policy or ARA Group's Employee Privacy Policy. Employees acknowledge that privacy in relation to any activity undertaken using AILM will be limited to the extent ARA Group has the right to monitor, access, retrieve, read and/or delete communications, information or data as contained in section 7 of this Policy.

4 Acceptable use of Artificial Intelligence Language Models

4.1 Employees are authorised to use AILM for work-related purposes, including generating text or content for reports, emails, presentations, images and communications.

4.2 Employees must exercise good judgment to act responsibly and ethically when using AILM and must use such facilities in a manner that is lawful.

4.3 AILM must not be used for the purposes of causing detriment to ARA Group or others.

4.4 Employees must, at all times, adhere to copyright laws, including but not limited to the *Copyright Act 1968* (Cth), when using AILM.

4.5 All information generated by AILM must be reviewed and edited by Employees for accuracy prior to any use.

4.6 Employees must follow all applicable data privacy laws and ARA Group policies when using AILM.

4.7 Employees must, at all times, comply with the terms and conditions (or contractual obligations) of usage of technology equipment and software of other parties (for example, Microsoft) and must otherwise comply with ARA Group's External Software Policy.

5 Prohibited conduct

5.1 Under no circumstances whatsoever are Employees to use AILM in any way which:

(a) is, or may reasonably be, considered to be offensive, abusive, racist, discriminatory, harassment, sexually explicit (including pornographic or generally distasteful in nature) and/or illegal;

(b) might encourage or promote activities which make unproductive use of ARA Group's time;

(c) might affect, or have the potential to affect, the performance of, damage, or overload ARA Group's IT Facilities in any way;

(d) is or may be defamatory or otherwise result in ARA Group and/or the individual incurring liability, or otherwise has an adverse impact on ARA Group's reputation;

(e) breaches copyright or other intellectual property protections – if an Employee is unsure whether a particular use of AILM constitutes copyright infringement, they should contact the ARA Group's Legal Department for guidance; or

(f) breaches an Employee's employment contract, ARA Group's Code of Conduct Policy, any other policy of ARA Group, or the law generally.

5.2 Confidential or commercially sensitive information must not be entered into an AILM tool, as such information may enter the public domain.

5.3 ARA Group does not accept responsibility for information distributed using AILM that does not comply with this Policy.

6 Risks of using Artificial Intelligence Language Models

6.1 Employees must at all times, and in particular when using AILM, be aware of the following risks (amongst others) associated with such use:

(a) any information entered into AILM may enter the public domain, which may:

(i) result in the unintentional release of confidential or commercially sensitive information into the public domain;

(ii) be in breach of legislative and regulatory requirements;

(iii) be in breach of client contracts; and/or

(iv) comprise ARA Group's trade secrets;

(b) any information generated by an AILM may be inaccurate or unreliable and therefore Employees must always review and edit responses for accuracy prior to using any generated content;

(c) AILM may produce content that is biased, discriminatory or offensive in nature and which may be in breach of this Policy; and

(d) AILM may store sensitive data and information, which could be at risk of cyber attack.

7 Monitoring of use of AILM and IT Facilities

7.1 Employees must only use AILM in accordance with this Policy.

7.2 ARA Group has the right to access, retrieve, read and delete any communication or information that is created or stored on, received through, or sent using IT Facilities, within the scope of applicable laws. This includes documents and personal emails, including those which have been deleted and otherwise exist in archives or backup storage systems.

7.3 To the extent permitted by law, ARA Group may conduct surveillance of Employees' of its IT Facilities, including personal mobile devices used for ARA Group business activities. Surveillance is conducted for various purposes, including but not limited to investigating suspected unlawful conduct or breaches of an Employee's obligations under this Policy, ARA Group's Code of Conduct or any other ARA Group policy, disciplinary or security purposes, or for other purposes concerning the protection of ARA Group's business and interests.

7.4 Surveillance may consist of recording, storing, tracking and monitoring the use of IT Facilities. Information concerning computer usage will be recorded onto the computer's hard drive and ARA Group's backup data stores. This information may be accessed and monitored by ARA Group using software and any other equipment.

7.5 ARA Group may use monitoring software to check the use and content of data transmitted through IT Facilities (including email and SMS).

7.6 The type of surveillance referred to above in sections 7.3 to 7.5 may be conducted on a continuous and ongoing basis throughout the course of the Employees employment and/or on demand in accordance with a request under section 7.8. Such surveillance may occur without notice to Employees where permitted by the law.

7.7 The Surveillance may include, without limitation, accessing, reviewing and auditing:

(a) email accounts and current, archived or deleted emails on ARA Group's servers;

(b) current, archived or deleted files on local, hard and share drives;

(c) work computers;

(d) internet usage records (including sites and pages visited, files downloaded, video and audio files accessed, and data input); and

(e) records of phone usage, including landline, mobile device and SMS.

7.8 Where ARA Group has reasonable suspicion to believe that an Employee is using AILM or IT Facilities in a manner that is contrary to the terms of use set out in this Policy, a surveillance review may be conducted (with written notice, as applicable) to examine the Employee's historical use of AILM or IT Facilities (**Surveillance Review**). The manager or supervisor of the Employee in question will be required to complete a Request for Surveillance Review (**Surveillance Request**) (available on request from ARA Group's Legal Department) setting out the reasons for the Surveillance Request and the IT Facilities to be reviewed. The Surveillance Request must be approved by the Employees' Divisional Managing Director, and by either ARA Group's Chief Executive Officer or Chief Financial Officer before the Surveillance Review can be conducted. Where a Surveillance Review is considered time critical, the IT Department may 'quarantine' the Employees' IT Facilities immediately and only release the information once approval of the Surveillance Request has been received. Notwithstanding the right to conduct a Surveillance Review contained in this section 7.8, a Surveillance Request may be refused where the Surveillance Request (without limitation):

(a) is frivolous or vexatious;

(b) does not adequately identify the reason(s) for the Surveillance Request or the particular IT Facilities to be reviewed;

(c) would infringe upon ARA Group's obligations under the *Privacy Act 1988* (Cth); or

(d) does not warrant sufficient reason to grant a Surveillance Review.

7.9 ARA Group may block an Employee's access to certain internet websites and otherwise prevent emails from entering or leaving their respective email systems, including where such websites or emails are offensive, inappropriate, non-work-related, or wasteful of electronic resources.

7.10 Where permitted by law, surveillance records may be used by ARA Group for disciplinary purposes.

8 Data collection and usage

Personal data collected from Employees for business processes in accordance with this Policy shall be protected from unauthorised access.

9 Compliance with laws

9.1 ARA Group will comply with all applicable laws in creating, maintaining and enforcing this Policy, including those concerning privacy and workplace surveillance.

9.2 Any contraventions of this Policy should be reported to the ARA Group's Legal Department.

10 Training and communication

ARA Group regularly communicates this Policy to Employees across ARA Group through its established communications channels. Employees may receive training supporting this Policy from time to time in the tenure of their employment with ARA Group.

11 Indemnity

Any Employee subject to this Policy agrees to indemnify ARA Group for any direct losses or reasonably foreseeable consequential losses suffered as a result of the Employee's breach of this Policy.

12 Disciplinary action

Alleged breaches of this Policy will be reviewed on a case-by-case basis and may be subject of disciplinary action, including but not limited to suspension and termination of employment, if appropriate in the circumstances. Notwithstanding this, any breach of this Policy may result in ARA Group commencing proceedings against an Employee.

Edward Federman
Chief Executive Officer

12 December 2023
Date