ACCEPTABLE USE OF INFORMATION TECHNOLOGY POLICY

ARA Group Limited ABN 47 074 886 561 and its related corporate entities (collectively **ARA Group**) are committed to managing operational risks, including maintaining appropriate measures to ensure company technology is used appropriately and for legitimate business purposes.

1 Purpose

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

(a) outline the acceptable use of the internet, email (including instant messaging), telephone (including mobile devices, text messaging and voicemail), social media, computers (including desktops, laptops and tablets), software applications, information systems, networks and infrastructure (including local and shared drives) and information technology facilities of ARA Group, irrespective of whether services are hosted within ARA Group's own infrastructure or hosted off premise as a managed cloud service (collectively **IT Facilities**);

(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, loss of intellectual property, and legal liability; and

(c) put Employees on notice that certain IT Facilities may be subject to surveillance by ARA Group.

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 IT Facilities which may adversely affect ARA Group or ARA Group's confidence and trust in its Employees.

2.3 Where Employees have opted-in to use an approved personal mobile device in connection with their ARA Group employment, this Policy will apply to the use of such device, and the definition of IT Facilities will extent to include personal mobile devices insofar as they are used to conduct ARA Group business and/or to exchange ARA Group data and information.

3 Proprietary rights

IT Facilities are the property of ARA Group (except personal mobile devices used for ARA Group business as above at subsection 2.3) and are to be used in the course of employment for business purposes in serving the interests of ARA Group. Any data created by Employees using IT Facilities remains the property of ARA Group.

4 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 IT Facilities 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 13 of this Policy.

5 Acceptable use of IT Facilities

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

5.2 Employees must not take advantage of IT Facilities for the personal gain of themselves or others, nor are IT Facilities to be used for the purposes of causing detriment to ARA Group or others.

5.3 Under no circumstances are IT Facilities to be destroyed or materially altered by any Employee without prior express authorisation from a proper officer of ARA Group, which for the avoidance of doubt includes a member of ARA Group's information technology department (**IT Department**).

5.4 Employees must not use IT Facilities for personal use in any way that could interfere with the responsibilities of the Employee, disrupt any technological system, or harm ARA Group's reputation.

5.5 Employees may not reallocate or swap equipment, systems or telephones with other employees unless prior permission has been given by ARA Group's IT Department.

5.6 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.

6 Prohibited conduct

6.1 Under no circumstances whatsoever are Employees to use any of the IT Facilities to; access, upload, download, use, retain, distribute or disseminate any images, text, materials or software which:

(a) are, or may reasonably be, considered to be offensive, abusive, racist, discriminatory, harassment, sexually explicit (including of a pornographic or generally distasteful 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 the IT Facilities in any way;

(d) are 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 (for example, copying copyrighted material such as software or photographs without proper authorisation); 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.

6.2 Employees must not store any information of ARA Group or its clients on any non-approved external resource or storage facility such as personal hard drives, USB storage, Gmail, Dropbox or iCloud.

6.3 ARA Group does not accept responsibility for information distributed using IT Facilities that does not comply with this Policy.

7 Use of internet

7.1 Employees must take care when accessing, using and transmitting information through the internet and be aware of the risks involved in accessing insecure websites.

7.2 Employees must not access internet sites which contain or concern:

(a) sexually explicit or pornographic material, including material that is tasteless or offensive generally;

(b) criminal activity of any kind, including money laundering, illegal drugs and violence;

(c) intolerance and hate;

(d) gambling and games;

(e) ringtones and mobile phone downloads;

(f) personal matters such as dating sites;

(g) hacking, spam URLs, spyware, phishing and fraud;

(h) soliciting or conducting business other than the business of ARA Group; or

(i) using, storing and/or transmitting any confidential or sensitive client information or internal information via an external website, internet file sharing programme or cloud service application without appropriate security controls in place.

7.3 ARA Group may block access to certain internet sites and will review and update prohibited sites as necessary.

8 Use of Social Media

8.1 ARA Group recognises the benefits of using social media for business purposes as a tool for communication and collaboration. This section 8 applies to social networking sites, video and photo sharing websites, micro-blogging and activity stream sites, blogs and blogging platforms, forums and discussion boards, online encyclopedias and any other websites which allow individual users or companies to use simple publishing tools (collectively **Social Media**).

8.2 When using Social Media, Employees must:

(a) not comment on the activities of any part or division of ARA Group, or ARA Group as a whole, apart from providing factual information that is within the public domain, where Employees have the authority to make such comments;

(b) not make any comments or statements or give any views or opinions on behalf of ARA Group or any part of it;

(c) not divulge or leak any information about ARA Group or its clients that is confidential, sensitive, or otherwise within the interests of ARA Group and its clients to keep private;

(d) refrain from any making any comments or statements that are or have reasonable potential of being defamatory, offensive, abusive, of poor taste, insulting, or generally contrary to ARA Group's Equal Employment Opportunity and Anti-Discrimination Policy, and ARA Group's Bullying and Harassment Policy;

(e) not do or say anything which might reasonably bring ARA Group into disrepute;

(f) not commit ARA Group or any part of it to any action or initiative without the appropriate authority to do so;

(g) not do anything which breaches the copyright or intellectual property of any person or company;

(h) uphold ARA Group's values and act with integrity, respect and courtesy;

(i) take reasonable steps to avoid conflicts of interest; and

(j) be apolitical, impartial and professional.

9 Use of email

9.1 ARA Group provides an email system to support its activities and access to the system is granted to Employees on this basis. When using email, Employees must take care generally and not do anything contrary to this Policy, including but not limited to acting in a wilful, reckless or negligent manner which could reasonably have an adverse effect on ARA Group or otherwise be or result in a contravention of this Policy.

9.2 Email accounts not provided by ARA Group (including personal email accounts) should not be used to conduct ARA Group business, and employees are not permitted to forward ARA Group email to non-ARA Group email addresses.

9.3 Emails form part of ARA Group's business records and may be subject to public disclosure as a result of legal action or regulatory investigations, amongst other reasons.

9.4 Professional language suitable for business must always be used and email correspondence must be polite, courteous and respectful. Defamatory language or statements must be avoided. Where possible, emails should contain the ARA Group signature with the name and title of the Employee sending the email(s).

9.5 Emails should not be used to send highly sensitive or confidential information unless appropriate security measures have been taken, such as password encryption.

9.6 Employees must not attempt to read the emails of other Employees or interfere with such emails unless express permission is given by the other person. Unauthorised use or forging of email header information is prohibited.

9.7 Employees must not deliberately or recklessly introduce any form of computer virus via email or send unsolicited bulk emails.

9.8 Employees should use extreme caution when opening email attachments received from unknown senders as they may contain viruses or other malicious codes.

10 Use of voice and conferencing systems

10.1 When using ARA Group voice or conferencing (including landline telephones, mobile devices such as mobile phones and smart phones, associated services such as voicemail and short-message service (**SMS**), video conference facilities or other meeting and conferencing services), Employees must adhere to professional standards of behaviour and business communication etiquette applicable in the region where they are working.

10.2 Employees are responsible for all use and activity associated with their mobile devices.

10.3 At a minimum, mobile devices must be protected by a password or personal identification number (**PIN**). Information stored on those devices should be kept to the minimum required to allow efficient out-of-office working.

10.4 Employees should avoid excessive use of mobile devices for business purposes where cheaper alternative means of communication are readily available. Excessive charges relating to the use of mobile devices for personal reasons may be passed from ARA Group to the Employee, who may also be subject to disciplinary action if appropriate.

10.5 Voice and conferencing systems should not be used for inappropriate purposes, including but not limited to:

(a) unlawful activities or wrongful acts generally;

(b) commercial purposes which are not related to ARA Group;

(c) in pursuit of personal financial gain by the Employee;

(d) calling or using services that are not appropriate to ARA Group's business, such as gambling, entertainment websites, and chat lines; and

(e) capturing and storing inappropriate content via camera phone.

10.6 Mobile devices must not be used while driving. ARA Group discourages the use of hands-free devices whilst driving, even where permissible by applicable laws.

11 Use of computer (including desktop and laptop)

11.1 Only ARA Group approved and licensed software is to be installed on Employees' computers. Employees who require a specific software package, application or upgrade for business purposes must first contact ARA Group's IT Department to ensure adherence to any software licensing obligations and not attempt to download or install any files from the internet or elsewhere. Employees will be held responsible for use of unlicensed software. Only ARA Group's approved hardware is to be connected to Employees' computers.

11.2 Employees must not modify any security protections or restrictions placed on their computers, applications and files.

11.3 Business related data must be stored on appropriate network drives, which are regularly backed up.

12 Security of IT Facilities

12.1 Employees must use only those IT Facilities and information which they have been authorised to use and access.

12.2 Passwords set by ARA Group or Employees to use any IT Facilities are to be treated as confidential and are not to be released to anyone (including Employees' manager or family members) nor written down or stored online. Password security is the responsibility of every individual Employee.

12.3 From time to time, ARA Group may impose Multi-Factor Authentication (**MFA**) access requirements upon IT Facilities which will require users to complete additional verification steps prior to accessing IT Facilities subject to MFA. The MFA access requirements may be changed by ARA Group at any time.

12.4 Employees are to take reasonable precautions to avoid loss, theft or damage to portable IT Facilities and must report loss immediately. Repeated instances of loss, theft or damage will be investigated and may result in disciplinary action. In the case of negligence, such as leaving IT Facilities unattended, the responsible Employee may be required to reimburse ARA Group for the cost of replacing an item or repairing a damaged item.

12.5 Where an Employee becomes aware of a security threat or reasonably perceived threat to IT Facilities, such as spam distributed by email, Employees should as soon as reasonably practicable report such security threats to ARA Group's IT Department.

13 Monitoring of IT Facilities

13.1 Employees must only use IT Facilities and information which they have been authorised to use and access.

13.2 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.

13.3 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.

13.4 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.

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

13.6 The type of surveillance referred to above in sections 13.3 to 13.5 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 13.8. Such surveillance may occur without notice to Employees where permitted by the law.

13.7 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.

13.8 Where ARA Group has reasonable suspicion to believe that an Employee is using 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 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 13.8, 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.

13.9 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.

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

14 Data collection and usage

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

15 Return and redistribution of IT Facilities

15.1 Any surplus equipment or equipment that ceases to be used by Employees (including where an Employee ceases to be employed by ARA Group for any reason), should be returned as soon as is practicable to the applicable Employee's manager or supervisor, or where in the circumstances it is reasonably convenient, to ARA Group's IT Department.

15.2 Where an Employee ceases to be employed by ARA Group for any reason, the Employee's manager or supervisor must ensure that the exiting Employee's access to IT Facilities is terminated immediately.

15.3 For the avoidance of doubt, should any uncertainty arise as to whom to return equipment to in accordance with this section 15, the applicable manager or supervisor of the Employee returning equipment is to be consulted.

15.4 Where IT Facilities are returned as set out in this section 15, ARA Group's IT Department shall do all things reasonably necessary to ensure file security and maintain software licensing adherence prior to redistributing IT Facilities.

16 Ownership

Any IT Facilities made available for Employee use by ARA Group are and shall remain in all circumstances the legal and beneficial property of ARA Group, notwithstanding ARA Group entrusting temporary possession of IT Facilities to Employees for the tenure of their employment with ARA Group.

17 Compliance with laws

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

18 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.

19 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.

20 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