INTERNET, EMAIL AND COMPUTER USE POLICY

1. PURPOSE

1.1 This Internet, Email and Computer Use Policy ('Policy') sets out the standards of behaviour expected of persons using Hope Diving Services Australia Pty Ltd ('HDSA Group')'s computer facilities, or when making reference to HDSA Group on external sites.

2. COMMENCEMENT OF POLICY

2.1 This Policy will commence from 08/11/2021. It replaces all other policies relating to use of HDSA Group's computers, internet, and email facilities (whether written or not).

3. APPLICATION OF POLICY

3.1 This Policy applies to all people who use HDSA Group's computer network by any means ('users'). The Policy also applies to users who contribute to external blogs and sites that identify themselves as associated with HDSA Group.

3.2 This Policy also sets out the type of surveillance that will be carried out in HDSA Group's workplace, relating to the use of HDSA Group's computer network.

3.3 This Policy does not form part of any employee's contract of employment. Nor does it form part of any other user's contract for service.

4. DEFINITIONS

4.1 In this Policy:

(a) 'Blogging' means the act of using web log or 'blog'. 'Blog' is an abbreviated version of 'weblog' which is a term used to describe websites that maintain an ongoing chronicle of information. A blog is a frequently updated website featuring diary-style commentary, audio-visual material and links to articles on other websites.

(b) 'Confidential information' includes but is not limited to trade secrets of HDSA Group; non-public information about the business and affairs of HDSA Group such as: pricing information such as internal cost and pricing rates, production scheduling software, special supply information; marketing or strategy plans; exclusive supply agreements or arrangements; commercial and business plans; commission structures; contractual arrangements with third parties; tender policies and arrangements; financial information and data; sales and training materials; technical data; schematics; proposals and intentions; designs; policies and procedures documents; concepts not reduced to material form; information which is personal information for the purposes of privacy law; and all other information obtained from HDSA Group or obtained in the course of working or providing services to HDSA Group that is by its nature confidential.

(c) 'Computer surveillance' means surveillance by means of software or other equipment that monitors or records information input or output, or other use, of HDSA Group's computer network (including, but not limited to, the sending and receipt of emails and the accessing of websites).

(d) 'Computer network' includes all HDSA Group's internet, email and computer facilities which are used by users, inside and outside working hours, in the workplace of HDSA Group (or a related corporation of HDSA Group) or at any other place while performing work for HDSA Group (or a related corporation of HDSA Group). It includes, but is not limited to, desktop computers, laptop computers, Blackberrys, Palm Pilots, PDAs, other handheld electronic devices, smart phones and similar products, and any other means of accessing HDSA Group's email, internet and computer facilities, (including, but not limited to, a personal home computer or personal electronic devices such as iPads, Tablets, Blackberrys, Palm Pilots, PDAs, other personal handheld electronic devices, smart phones and similar products which have access to HDSA Group's IT systems).

(e) 'Intellectual property' means all forms of intellectual property rights throughout the world including copyright, patent, design, trade mark, trade name, and all confidential information and including know-how and trade secrets.

(f) 'Person' includes any natural person, company, partnership, association, trust, business, or other organisation or entity of any description and a person's legal personal representative(s), successors, assigns or substitutes.

5. USE OF INTERNET, EMAIL AND COMPUTERS

5.1 Users are entitled to use HDSA Group computer network only for legitimate business purposes.

5.2 However, users are permitted to use HDSA Group's computer network for limited and reasonable personal use. Any such personal use must not impact upon the user's work performance or HDSA Group resources or violate this Policy or any other HDSA Group Policy.

5.3 A user must not use HDSA Group's computer network for personal use if that use interferes with the efficient business operations of HDSA Group or relates to a personal business of the user.

5.4 HDSA Group gives no warranty or assurance about the confidentiality or privacy of any personal information disclosed by any user in the course of using the computer network for the user's personal purposes.

6. REQUIREMENTS FOR USE

6.1 Users must comply with the following rules when using HDSA Group's computer network.

(a) Users must use their own username/login code and/or password when accessing the computer network.

(b) Users in possession of HDSA Group's electronic equipment must at all times handle the equipment in a responsible manner and ensure that the equipment is kept secure.

(c) Users should protect their username/login code and password information at all times and not divulge such information to any other person, unless it is necessary to do so for legitimate business reasons.

(d) Users should ensure that when not in use or unattended, the Computer System is shut down.

(e) A disclaimer is automatically included in all HDSA Group emails, and must not be removed.

(f) If a user receives an email which the user suspects contains a virus, the user should not open the email or attachment to the email and should immediately contact the IT Department for assistance.

(g) If a user receives an email the content of which (including an image, text, materials or software) is in breach of this Policy, the user should immediately delete the email and report the matter to the IT Department. The user must not forward the email to any other person.

7. PROHIBITED CONDUCT

7.1 Users must not send (or cause to be sent), upload, download, use, retrieve, or access any email or material on HDSA Group's computer network that:

(a) is obscene, offensive or inappropriate. This includes text, images, sound or any other material, sent either in an email or in an attachment to an email, or through a link to a site (URL). For example, material of a sexual nature, indecent or pornographic material;

(b) causes (or could cause) insult, offence, intimidation or humiliation;

(c) may be defamatory or could adversely impact the image or reputation of HDSA Group. A defamatory message or material is a message or material that is insulting or lowers the reputation of a person or group of people;

(d) is illegal, unlawful or inappropriate;

(e) affects the performance of, or causes damage to HDSA Group's computer system in any way;

(f) gives the impression of or is representing, giving opinions or making statements on behalf of HDSA Group without the express authority of HDSA Group. Further, users must not transmit or send HDSA Group's documents or emails (in any format) to any external parties or organisations unless expressly authorised to do so.

7.2 Users must not use HDSA Group's computer network:

(a) to violate copyright or other intellectual property rights. Computer software that is protected by copyright is not to be copied from, or into, or by using HDSA Group's computing facilities, except as permitted by law or by contract with the owner of the copyright;

(b) in a manner contrary to HDSA Group's Privacy Policy;

(c) to create any legal or contractual obligations on behalf of HDSA Group unless expressly authorised by HDSA Group;

(d) to disclose any confidential information of HDSA Group or any customer, client or supplier of HDSA Group's unless expressly authorised by HDSA Group;

(e) to install software or run unknown or unapproved programs on HDSA Group's computer network. Under no circumstances should users modify the software or hardware environments on HDSA Group's computer network;

(f) to gain unauthorised access (hacking) into any other computer within HDSA Group or outside HDSA Group, or attempt to deprive other users of access to or use of any HDSA Group's computer network;

(g) to send or cause to be sent chain or SPAM emails in any format;

(h) to use HDSA Group's computer facilities for personal gain. For example, running a personal business.

7.3 Users must not use another user's computer network facilities (including passwords and usernames/login codes) for any reason without the express permission of the user or HDSA Group.

8. DETAILS ON BLOCKING EMAIL OR INTERNET ACCESS

8.1 HDSA Group reserves the right to prevent (or cause to be prevented) the delivery of an email sent to or from a user, or access to an internet website by a user, if the content of the email or the internet website is considered:

(a) obscene, offensive or inappropriate. This includes text, images, sound or any other material, sent either in an e-mail message or in an attachment to a message, or through a link to an internet website (URL). For example, material of a sexual nature, indecent or pornographic material;

(b) causes or may cause insult, offence, intimidation or humiliation;;

(c) defamatory or may incur liability or adversely impacts on the image or reputation of HDSA Group. A defamatory message or material is a message or material that is insulting or lowers the reputation of a person or a group of people;

(d) illegal, unlawful or inappropriate;

(e) to have the potential to affect the performance of, or cause damage to or overload HDSA Group's computer network, or internal or external communications in any way;

(f) to give the impression of or is representing, giving opinions or making statements on behalf of HDSA Group without the express authority of HDSA Group.

8.2 In the case that an email is prevented from being delivered to or from a user, the user will receive a prevented delivery notice. The notice will inform the user that the delivery of the email has been prevented. The notice will not be given if delivery is prevented in the belief that:

(a) the email was considered to be SPAM, or contain potentially malicious software; or

(b) the content of the email (or any attachment) would or might have resulted in an unauthorised interference with, damage to or operation of any program run or data stored on any of HDSA Group's equipment; or

(c) the email (or any attachment) would be regarded by a reasonable person as being, in all the circumstances, menacing, harassing or offensive.

8.3 HDSA Group is not required to give a prevented delivery notice for any email messages sent by a user if HDSA Group is not aware (and could not reasonably be expected to be aware) of the identity of the user who sent the e-mail or is not aware that the e-mail was sent by the user.

9. Type of surveillance in **HDSA GROUP**'s workplace

9.1 On a continuous and ongoing basis during the period of this Policy, HDSA Group will carry out computer surveillance of any user at such times of HDSA Group's choosing and without further notice to any user.

9.2 Computer surveillance occurs in relation to:

(a) storage volumes;

(b) internet sites — every web site visited is recorded including the time of access, volume downloaded and the duration of access;

(c) download volumes;

(d) suspected malicious code or viruses;

(e) emails — the content of all emails received, sent and stored on the computer network (this also includes emails deleted from the Inbox); and

(f) computer hard drives — HDSA Group may access any hard drive on the computer network.

9.3 HDSA Group retains logs, backups and archives of computing activities, which it may audit. Such records are the property of HDSA Group, are subject to State and Federal laws and may be used as evidence in legal proceedings, or in workplace investigations into suspected misconduct.

10. WHAT WILL THE COMPUTER SURVEILLANCE RECORDS BE USED FOR?

10.1 HDSA Group may use and disclose the computer surveillance records where that use or disclosure is:

(a) for a purpose related to the employment of any employee or related to HDSA Group's business activities; or

(b) use or disclosure to a law enforcement agency in connection with an offence; or

(c) use or disclosure in connection with legal proceedings; or

(d) use or disclosure reasonably believed to be necessary to avert an imminent threat of serious violence to any person or substantial damage to property.

10.2 For example, use or disclosure of computer surveillance records can occur in circumstances of assault, suspected assault, theft or suspected theft of HDSA Group's property (or that of a related corporation of HDSA Group) or damage to HDSA Group's equipment or facilities (or that of a related corporation of HDSA Group).

11. STANDARDS IN RELATION TO BLOGS AND SITES NOT OPERATED BY HDSA Group

11.1 HDSA Group acknowledges that users have the right to contribute content to public communications on websites not operated by HDSA Group, such as social networking sites like LinkedIn, Facebook or YouTube. However, inappropriate use of such communications has the potential to cause damage to HDSA Group, employees, clients and suppliers. For that reason, the following provisions apply to all users:

(a) As it may be possible for any user of an external site to conduct a search that will identify any comments about HDSA Group, users must **not** publish any material which identifies themselves as being associated with HDSA Group, except in the case of appropriate postings on LinkedIn.

(b) Users must not publish any material that may expose HDSA Group to any possible legal liability. Examples include, but are not limited to, defamation or discrimination proceedings.

(c) If it comes to HDSA Group's attention that a user has made inappropriate and/or unauthorised comments about HDSA Group or a HDSA Group employee, or HDSA Group contractor, HDSA Group may choose to take disciplinary action against a user as outlined in this Policy.

12. WARNING

12.1 Apart from the potentially damaging effects a blog or post may have on HDSA Group, inappropriate blogs or posts on internal or external sites can also have adverse consequences for a user in terms of future career prospects, as the material remains widely and permanently accessible to other site users.

13. USE OF PERSONAL COMPUTERS AND ELECTRONIC DEVICES

13.1 This Policy applies to the use of personal computers, personal electronic devices such as iPads, Tablets, Blackberrys, Palm Pilots, PDAs and other personal handheld electronic devices, smart phones and similar products which have

access to HDSA Group's IT systems, to the extent that such use may damage HDSA Group's business interests and employment relationships, whether this occurs during working hours or not.

14. ENFORCEMENT

14.1 Users must comply with the requirements of this Policy. Any breach of this Policy may result in disciplinary action which may include termination of employment (or, for persons other than employees, the termination or non-renewal of contractual arrangements).

14.2 Other disciplinary action that may be taken includes, but is not limited to, issuing a warning, suspension or disconnection of access to all or part of HDSA Group's computer network whether permanently or on a temporary basis.

Variations

HDSA Group reserves the right to vary, replace or terminate this Policy from time to time.