Technology and Social Media Policy

1 Policy Objectives

1.1 The purpose of this Policy is intended to clearly define the conditions of use of Technology, Internet and Social Media when working at the Company.

(a) The Company provides access to vast information resources and facilities of the internet to help you do your job faster and more efficiently to assist in ensuring the latest available data and technology is used.

(b) The use of company computers, email and internet facilities must be conducted in a manner that does not breach the principles of this policy or other relevant policy.

(c) Whether you are handling a corporate social media account or using your own, you should remain productive and avoid damaging our organisation in any way. This policy provides practical advice to avoid issues that might arise by careless use of social media in the workplace.

(d) If you breach any of the provisions of this Policy, then we may take disciplinary action against you.

(e) This Policy may be changed and updated in response to changing circumstances as Internet and email facilities develop, whether operational or legislative.

2 Scope & Application

2.1 This Policy applies to all employees.

2.2 This policy is built around two different elements: firstly, appropriate usage of technology in the workplace and. secondly, using personal social media and representing our company through social media.

2.3 Technology refers to laptops, desktops, tablets, phones, printers, smart watches, and other smart electronic devices as well as online systems i.e., video conferencing, emails, Microsoft Teams etc.

2.4 Social Media refers to a variety of online communication communities including blogs, social networks, chat rooms, forums, video/photo sharing sites, micro-blogs, wikis, podcasts, and geo- spatial tagging (for example, Facebook check-ins).

3 Potential Problems

Our image

3.1 We must all take special care to maintain the clarity, consistency, and integrity of our image. Anything any employee writes in an email from our system, on a social media post or published on other online platforms could be construed as representing the Company. This presents some significant risks for us and to you.

The law

3.2 There is also a danger that, if our email system or Internet access is abused, we may be found to have broken the law. That could result in criminal penalties or our having to pay damages (for example in respect of harassment).

Viruses

3.3 Other problems that might arise include importing viruses onto our systems or hardware.

4 Technology

Personal Use of technology in the workplace

4.1 The use must be of a limited and of a reasonable nature:

(f) Personal use of either company or personal computer, email and internet facilities must not in any way interfere with the proper discharge of an employee's duties and must not interfere with other staff members performing their work duties.

(g) Any personal use must be in accordance with this and other relevant Company policies.

(h) Staff members must not use Company computer, email, and internet resources for inappropriate purposes.

(i) You should use the internal email system for the purposes of our organisation only.

(j) You must not send or distribute jokes, comic material, or material of an offensive, obscene, or malicious nature to colleagues – as you risk offending colleagues and wasting your and their time during business hours.

(k) We expect you to adhere to our confidentiality policies at all times and to avoid violating our anti-harassment policies or sharing something that might make your collaboration with your colleagues more difficult (e.g., hate speech against groups where colleagues belong).

4.2 Any personal calls or texts should only be responded to if it is an emergency. Employees should restrict personal calls by using their personal computer or mobile phone only during scheduled breaks or lunch periods.

4.3 To ensure compliance with the Company's internal policies as well as applicable laws and regulations, and to ensure employee safety, the Company reserves the right to monitor, inspect, and/or search at any time all the Company's information systems.

4.4 The use of email, internet and computers by staff members may be subject to surveillance and monitoring on an ongoing basis available to the Company, including by way of accessing, reviewing, and monitoring all data and messages stored, sent or received over Company electronic communication systems (including email and internet) or on the computers. For the avoidance of doubt, this policy constitutes notice of surveillance for the purposes of applicable workplace surveillance legislation. Further details can be found at Section 8 Surveillance of this policy.

4.5 The Company information systems that may be subject to such surveillance include, but are not limited to, computers, electronic mail system files, social media accounts, personal computer hard drive files, voicemail files and printer spool files.

4.6 Since Company computers and networks are provided for business purposes as a work tool, the Company retains the right to remove from its information systems any material it views as offensive or potentially illegal.

4.7 The Company will endeavour to respect the privacy of staff members communications. However, you should be aware of the following:

(a) use of email and internet will be monitored to ensure compliance with this policy. This monitoring may bring to light actual, or suspected, breaches of this policy.

(b) communications will be viewed if it comes to the attention of the Company that a staff member has been (or may have been) using email and internet facilities in a manner contrary to this policy. This includes communications sent for business or personal purposes.

(c) any communications sent, received, or stored by staff members using the network facilities are the property of the Company not of the staff member.

(d) copies of all email communications may be stored in back up files, irrespective of whether a staff member has personally deleted email from his or her account.

(e) Email is discoverable in legal proceedings and the Company is obligated by law to retain copies of email for a period of time.

(f) Email communications and logs of internet activity may be viewed where necessary.

Security

4.8 The Company has installed a variety of firewalls, proxies, Internet address screening programmes and/or other security systems to assure the integrity, safety and security of the Company's network and to limit access to certain sites. You must not attempt to disable, defeat or circumvent these systems.

4.9 As set out above, passwords are an important aspect of security. Employees should not share passwords or record passwords in writing.

5 Internet guidelines

5.1 Under no circumstances should any staff member possess, access, display, archive, edit, record, use, view, send, store or download any type of material, through use of Company internet that:

(a) is fraudulent;

(b) is harassing, abusive, threatening or intimidating, or which could constitute bullying, or which does, or potentially, affects the health or safety of another person;

(c) contains material that could be considered to negatively reflect upon a particular race, gender, religion, colour, national origin, disability, sexual preference, or marital status;

(d) is sexually explicit, profane, or obscene (including, but not limited to, pornography of any kind, or material which is associated with the exploitation of children in any form);

(e) is related in any way to terrorist activity or could be seen to suggest support of such activities;

(f) is destructive to the Company's computing facilities or reputation;

(g) criticises the Company or any of its employees;

(h) is defamatory;

(i) infringes copyright;

(j) is pirated;

(k) any reasonable person might consider to be offensive;

(l) is competitive with the business of the Company or is connected to a business that is not related to the Company;

(m) does not comply with this Policy; or

(n) is unlawful (or potentially unlawful).

5.2 Breach of this clause may lead to disciplinary action being taken against the staff member.

Receipt of Offensive Material

5.3 If a staff member receives an email or a message that they consider to be inappropriate or offensive from a person within the Company, in the first instance, we ask that you delete the email and request the sender not to send such material again. Often the sender may not realise the communication is inappropriate or offensive.

5.4 If the person continues to send emails that are inappropriate or offensive, or the material which has been sent is considered to be illegal or seriously offensive (for example, the email is part of a bullying or harassment campaign, or contains sexually explicit images, or pornography), the staff member should immediately advise a director and or Human Resources.

5.5 If inappropriate or offensive material comes from a client, the matter should be raised with a director and/or Human Resources.

Copyright

5.6 Staff members must be mindful of not infringing copyright when they use email and the internet. The *Copyright Act 1968* (Cth) provides authors of literary, dramatic or musical works or the creators of artistic works with such exclusive rights as reproducing, publishing and communicating their works. It is an infringement of that copyright if someone exercises those rights without the permission of the owner.

5.7 Copyright can be infringed by using email or the internet in many ways. For example, by:

(a) downloading a copyrighted work without permission;

(b) posting a copyrighted work on a web site or bulletin board without permission; or

(c) emailing copyrighted works to others without permission.

5.8 Generally, personal research is permitted, but if copyrighted material is to be distributed to others or used for business purposes, staff members should ensure that they have the permission of the copyright owner.

6 Social Media

Social Media Responsibilities

6.1 This policy is made in contemplation of the Australian Rules of Racing (**Rules**), and employees must consider both the Rules and this Policy when making statements, posts or comments on any form of social media.

6.2 We respectfully ask that you do not use personal social media accounts during work time for personal interactions. We do encourage our employees to share and positively engage in posts initiated by the Company to build our company profile online, promote our values and culture to attract new clients and potential employees.

6.3 We ask you to be careful when posting on your personal social media. We expect you to adhere to our confidentiality policies at all times and to avoid violating our anti-harassment policies or posting something that might make your collaboration with your colleagues more difficult (e.g., hate speech against groups where colleagues belong).

6.4 We advise our employees to:

(a) Ensure others know that your personal account or statements don't represent our company. You shouldn't state or imply that your personal opinions and content are authorised or endorsed by our company. We advise using a disclaimer such as "opinions are my own" to avoid misunderstandings.

(1) We respectfully ask that you do not use personal social media accounts during work time.

(2) We ask you to be careful when posting on your personal social media.

(b) Avoid sharing intellectual property like trademarks on a personal account without approval. Confidentiality policies and laws always apply.

(c) Avoid any defamatory, offensive, or derogatory content. It may be considered as a violation of our company's anti-harassment policy, if directed towards colleagues, clients, or partners. Do not engage in any online conflict.

6.5 Please consider the points below (Representing our Company) when sharing or engaging with Company posts from your personal social media accounts.

Representing our Company

6.6 Some employees represent our company by handling corporate social media accounts or speak on our company's behalf. When you're sitting behind a corporate social media account, we expect you to act carefully and responsibly to protect our company's image and reputation.

6.7 You should:

(a) Be respectful, polite, and patient when engaging in conversations on our company's behalf.

(b) You should be extra careful when making declarations or promises to customers and stakeholders.

(c) Avoid speaking on matters outside your field of expertise when possible. Everyone should be careful not to answer questions or make statements that fall under somebody else's responsibility.

(d) Follow our Code of Conduct and observe laws on copyright, trademarks, plagiarism, and fair use.

(e) Never post discriminatory, offensive, or vilifying content and commentary.

(f) Follow the Australian Rules of Racing, and be conscious of joining any groups or online communities that act against the interests of the racing industry.

(g) Avoid deleting or ignoring comments for no reason, pass any comments needing a response to the Operations Manager.

(h) Correct or remove any misleading or false content as quickly as possible and pass miss information onto the Operations Manger

6.8 Please immediately notify the Operations Manager should you see any posts that negatively affect the company's image or reputation.

7 Surveillance

7.1 Legislation requires that employees be formally notified of any actions by their Company that fall within the definitions of surveillance. Notification must meet the fourteen (14) day requirement notice period stated in the Legislation, unless a shorter period is agreed to for existing employees. For the avoidance of doubt, this section of the policy constitutes notice of surveillance for the purposes of applicable workplace surveillance legislation. Surveillance under the Workplace Surveillance Act 2005 defines "Surveillance of an Employee" in the following ways:

7.2 **Surveillance of an employee means surveillance** of an employee by any of the following means:

(a) camera surveillance, which is surveillance by means of a camera that monitors or records visual images of activities on premises or in any other place,

(b) computer surveillance, which is surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, the sending and receipt of emails and the accessing of Internet websites),

(c) tracking surveillance, which is surveillance by means of an electronic device the primary purpose of which is to monitor or record geographical location or movement (such as a Global Positioning System tracking device).

Type of surveillance employed at the Company

7.3 The type of surveillance to be carried out is "Camera Surveillance" as defined in 8.2(a) above.

(a) Camera Surveillance has been installed for the purpose of increasing safety and security for staff and for the security of the business premises.

(b) Cameras have been installed at the offices.

(c) The camera surveillance will be continuous and ongoing.

(d) Cameras will be clearly visible, and signs will be displayed in areas where the surveillance will take place.

(e) The installed cameras will also record sound/voices.

(f) The type of surveillance to be carried out is "Computer Surveillance" as defined in (b) above.

(g) Computer Surveillance has been employed across our systems to maintain the safety and integrity of our computer systems.

(h) Computer Surveillance may be employed across all of our computer systems.

(i) The computer surveillance will be continuous and ongoing.

Disclosure of surveillance records

7.4 Any surveillance records made as a result of the surveillance will not be used or disclosed unless:

(a) They are for a legitimate purpose related to employment or business activities or functions;

(b) They are required to be presented to law enforcement agencies;

(c) They relate to civil or criminal proceedings;

(d) It is necessary in order to avert an imminent threat, serious violence to persons or substantial damage to property.

8 Disciplinary Consequences

8.1 The Company will monitor all social media postings on our corporate account. The Company reserves the right to monitor, inspect, and/or search at any time all the Company's information systems and any breaches found will result in investigation and disciplinary actions may apply.

8.2 We may have to take disciplinary action leading up to and including termination if employees do not follow this policy's guidelines.

8.3 Examples of non-conformity with the employee Technology + Social Media Policy include but are not limited to:

(a) Disregarding job responsibilities and deadlines to use social media at work.

(b) Disclosing confidential information through personal or corporate accounts.

(c) Directing offensive comments towards other members of the online community.

8.4 If you violate this policy inadvertently, you may receive a reprimand. We expect you to comply thereafter or stricter disciplinary actions will apply.