Information Technology Policy

1. Scope

This policy applies to anyone performing work (**you/workers**) for Sports Aid Pty Ltd (**Company**).

2. Purpose of this policy

It is essential that all of our workers that use our computers, email, internet and other systems adhere to certain guidelines, to ensure the safety and appropriateness of their use of information technology (**IT**) in the Company's workplace. This policy sets out:

- the responsibilities of the Company's workers who use our IT; and
- the Company's policy for acceptable and unacceptable use of IT.

3. Email usage

When using our email systems, you are making communications on both your own behalf, as well as on behalf of the Company. For this reason, it is vital that all the Company's workers communicate in a professional way both internally and externally, and otherwise comply with the terms of this policy when communicating with all parties through email.

Email may only be used for the following purposes in the Company's workplace:

- communications for work-related purposes within the Company;
- communications for work-related purposes with people outside the Company; and
- incidental and occasional personal use of email.

Unacceptable use of email amounts to a breach of this policy, and includes, but is not limited to:

- excessive personal use of email, or distribution of jokes, gossip and rumours;
- email which would be likely to offend, harass, insult or discriminate against any other person;
- abusive language;
- pornographic material;
- the dissemination of junk or chain mail;
- the distribution of information which infringes copyright laws;
- use for any illegal activity or purpose;
- distribution of confidential information to third parties without authorisation; and
  any other use which is inappropriate for the workplace.

All email transmissions sent and received through the Company's systems are the property of the Company, and administration of the Company's email systems is at the Company's sole discretion. If the Company considers that use of email systems in breach of this policy is occurring, it reserves the right to monitor email accounts and take appropriate action in line with this policy, including the recovery of any deleted communications.

The Company reserves the right to grant or remove email access to a worker at its discretion.

4. Internet

Workers may only use the internet on the Company's systems for:

- work-related purposes; and

- incidental and occasional personal use.

When using the internet on the Company's systems, or in the course of undertaking their duties, workers must not:

- access or disseminate any pornographic or illegal material;
- access or disseminate material which is defamatory, discriminatory, vilifying or harassing;
- engage in excessive personal or non-work-related use; and
- download any software without the express approval of the Company.

The Company monitors internet usage by its workers and may take appropriate action if it considers that use in breach of this policy is occurring.

5. Social media

Almost everyone uses social media, and it has relevant application to both the personal and professional lives of our workers. For this reason, it is necessary for the Company to implement restrictions on how its workers use social media, in relation to the Company. This policy applies to all social media usage of workers of the Company, including but not limited to the following platforms:

- social networking sites such as Facebook, Twitter and LinkedIn;
- media platforms such as Instagram and YouTube; and
- online blogs and forums.

When using social media you are required to:

- not use false or fake personas;
- not pretend to be an impartial individual in order to promote the company, its brand, products or services;
- not hold yourself out as a representative of the Company, or as expressing an opinion on behalf of the Company, without the express authorisation of the Company;
- refrain from undertaking any personal social media communication on matters that relate to the Company, or that may negatively affect the Company's reputation or business;
- not disseminate any confidential or proprietary information of the Company or any other third party;
- not make reference to clients, colleagues, suppliers or sub-contractors of the Company without their express prior approval;
- ensure your communications do not include prohibited material such as postings that may be considered discriminatory, offensive, harassing, pornographic or illegal; and
- inform management if any worker becomes aware of any negative comment made about the Company, its brand, products or services on any social media.

These guidelines apply to all workers, and any use of social media that is in breach of this policy will be addressed by the Company in accordance with this policy.

6. Security

All workers have a responsibility to ensure that they:

- keep any IT hardware, such as laptops and phones, safe and secure at all times while they are in the worker's possession, and to return such property as requested by the Company, or immediately on the end of their employment or engagement;
- keep all passwords for IT systems safe and secure at all times; and
- keep all confidential information of the Company, or any third party safe and secure, in their possession safe and secure.

Where a worker becomes aware of any security breach in relation to the above matters, they must immediately report this to their direct manager.

7. IT surveillance

The Company will carry out ongoing and intermittent IT surveillance and workers should have no expectation of privacy over their use of the Company's IT systems. This may include email filters, internet monitoring software and devices, and tracking devices, and any other similar surveillance methods permitted by the relevant legislation, and deemed appropriate by the Company, from time to time.

8. Contravening this policy

Any breach of this policy may lead to disciplinary action up to and including termination of employment or engagement as relevant.