Use of Information Technology System Policy

1. Purpose & Scope

This policy sets out guidelines for acceptable use of the internet, electronic communications (including email, client management systems, instant messaging and social media) and any other information technology systems (referred to as "the IT system") by APMHA HealthCare Ltd. staff.

This policy applies to all APMHA General Managers, employees and subcontractors (collectively referred to as "staff"), when they are working from APMHA offices, a home office or another location.

2. Policy

The primary purpose for providing staff with access to the IT system is to assist them in carrying out the duties of their employment. Staff may also use the IT system for reasonable private purposes that are consistent with this policy. Staff may not use the IT system in a way that significantly interferes with the duties of their employment or exposes APMHA to significant cost or risk of liability.

2.1 What is acceptable use

Subject to the balance of this policy, APMHA staff may use the IT system for:

- Work-related purposes
- For personal purposes as specified below, provided in each case that the personal use is moderate in time, does not incur significant cost for APMHA and does not interfere with the employment duties of the staff member or colleagues:
    - Sending and receiving personal email messages, provided that if email messages are sent with a company email address, the email contains a disclaimer to the effect that the sender's views may not represent those of APMHA.
    - Using instant messaging software and the internet for personal purposes

2.2 What is not acceptable use

Except in the course of an staff member's duties or with the express permission of APMHA, the IT system may not be used to:

- Share confidential information/material, trade secrets, or proprietary information outside of the organisation
- Disseminate information that is defamatory to the company, its products/services, employees, subcontractors, clients, service users and stakeholders
- Compromise the confidentiality of client information
- Disseminate personal contact information of APMHA employees, subcontractors, service users, clients and stakeholders without their consent
- Pass off personal views as representing those of the organisation
- Undertake any personal commercial or private business dealings
- Access gambling sites and sites that contain what a reasonable person would regard as obscene, hateful, pornographic, unlawful, or violent material, and any illegal material

- Perpetrate, or attempt to perpetrate, any form of fraud, theft, unauthorised access and/or software, film or music piracy
- Deliberately introduce malicious software that may affect company IT system or its users
- Disseminate, access or store images, material or information that may damage the organisation's reputation, result in victimisation or harassment, lead to any criminal penalty or civil liability, or be reasonably be found to be offensive or obscene. This includes:
    - images, material or information that is, or may reasonably found to be, defamatory, deceptive, harassing, threatening, obscene, offensive, discriminatory, sexist, racist or abusive (including comments about a person's sexual preferences, age, criminal or medical record, mental or physical condition)
    - images, material or information that breaches the Racial Discrimination Act 1975, the Sex Discrimination Act 1984, and the Disability Discrimination Act 1992
    - sexual comments, jokes or images or sexually explicit material of any kind
    - unsolicited bulk emails, chain letters, or promoting political, religious or lifestyle beliefs
- Create emails containing (or forwarding, attaching or containing links to) material that is or includes trademarks or copyrighted material of any person without specific authorisation to do so from the owner of the trademark or copyright
- Send an email in another person's name unless you have permission from that person
- Knowingly downloading or requesting software or media files or data streams that staff have reason to believe will use a greater amount of network bandwidth than is appropriate.

A staff member should consult their manager, if they are unsure about what constitutes acceptable IT system usage.

2.3 Consequences of unacceptable use

Individual staff members are responsible for their use of the IT system and complying with this Policy.

APMHA will review any alleged unacceptable use of the IT system on an individual basis. Any violation of this policy may result in disciplinary and/or legal action leading up to and including the termination of employment. Staff may also be held personally liable for damages caused by any violations of this policy.

APMHA has the right to keep and monitor IT system usage logs as a precaution to fraud, workplace harassment or breaches of confidence by staff. Staff have the right to be notified if their usage of the IT system is accessed. Usage logs may reveal information such as the internet servers (including websites) accessed by staff, and the email addresses of people they have contacted.

APMHA will not engage in real-time surveillance of IT system usage or monitor the content of email messages sent or received by its employees, unless a copy of such message is sent or forwarded to the company by its recipient or sender in the ordinary way. APMHA will not disclose any of the logged, or otherwise collected, information to a third party except under compulsion of law.

2.4 Security

All APMHA owned devices are protected with current anti-virus and automatic data back-up systems to ensure security and file protection and restoration in the event of computer malfunction.

Staff may access the IT system using personal devices such as mobile phones, tablets, laptops and desktops. If staff are using their own devices to access the IT system, they must ensure the device:

- is password protected and stored securely

- able to be erased remotely
- protected with a licenced anti-virus
- uses licenced software

2.5 Business documents

APMHA staff have access to a shared facility for storing and accessing company documents. Staff will store all business documents in this shared facility, with the exception of some confidential company information. The General Managers and CEO decide who has access to confidential company information.

Business documents are the exclusive property of APMHA HealthCare Ltd., whether prepared in whole or in part by staff. If a staff member ceases employment with APMHA HealthCare Ltd., they must relinquish all access to business documents and may not keep nor share outside the company any copies of business documents in any format.

3. Definitions

Information technology (IT)

The internet, electronic communications (including email, client record management, instant messaging and social media), document storage and other information technology systems provided by the APMHA HealthCare Ltd.

Confidential Information

Includes information that would reasonably be understood to be confidential in nature. This includes but is not limited to consumer records, commercial-in-confidence information or information that has been identified by its provider as being confidential.