INFORMATION TECHNOLOGY AND COMMUNICATIONS POLICY OF THE PRACTICE OF DR RUDI HAYDEN (referred to as "the practice")

This policy applies to all staff of the practice, on short term contracts and temporary staff

belonging to employment agencies.

1. Objective

This policy aims to regulate the use of information technology (referred to as "IT") and communications tools within the context of the practice. This policy defines the use of IT facilities of the practice.

2. Scope and application

2.1 This policy applies to all employees and contractors.

2.2 Specific notice must be taken to the rules below in relation to email communications, social media and cellphones. No expectation of privacy can exist where the Practice's IT and communications infrastructure is used for personal purposes.

3. Policy & procedures

3.1 Utilization of IT infrastructures:

3.1.1 IT infrastructure such as PC's (Hardware and software), laptops, networks, Internet access or the Practice telephone system are working tools for business purposes. The following regulations apply:

- 3.1.1.1 Private utilization of IT infrastructures must be kept to an absolute minimum. Exceptional personal use, such as when there is a family emergency or an emergency at home will be permissible. Limited personal email is permissible, provided that this is not excessive and does not interfere with the requirements of the practice and / or the duties of the employee. The practice may monitor all internet and e-mail usage from time to time and no employee has any expectation of privacy in this regard.

- 3.1.1.2 Any private utilization of IT infrastructures which is allowed does not mean that the employer allows, or would continue to allow such usage, in particular certain services may be restricted (e.g. no access to certain websites, no access to Facebook, Twitter, etc. during working hours, etc.).

- 3.1.1.3 All software installed on the practice's IT systems must be correctly licensed legally. No software other than that required for the operation of the practice may be downloaded. Should additional software be required, the permission of the practice must be obtained.

- 3.1.1.4 The practices IT security measures must not be deactivated. The deactivation of such security measures constitutes an infringement of the security regulations and can incur disciplinary action.

- 3.1.1.5 IT support will be arranged through the practice, and no employee may tamper with either the hardware or software associated with the practice's computers.

- 3.1.1.6 The practice reserves the right to at any stage block any website or sites it deems to be used for personal purposes or which is deemed undesirable within the work context.

- 3.1.1.7 Where a laptop is provided, this may only be removed from the premises of the practice with the express permission of the employer.

- 3.1.1.8 Where a remote internet card, such as through a mobile phone service provider, or another wireless provider, is provided, the employee may not remove the SIM card, or any part of the equipment, and may not use such card or wireless equipment for any purpose other than for what it is intended, and for practice purposes.

- 3.1.1.9 All emails have to include a standard disclaimer, which will include confidentiality and proprietary clauses, as well as a statement that any unintended receipt of an email must be lead to its destruction and that the sender has to be informed of such instance without delay. The disclaimer may be amended from time to time at the sole discretion of the practice and / or to keep place with applicable legislation.

3.1.2 All telephone and fax bills will be monitored, and the employee may be required to indicate personal calls on accounts received, and will be expected to pay for such calls at the cost indicated on the account. Where not paid in cash, the employee will sign an authorization that such amounts may be deducted from his / her salary.

3.1.3 The Practice's IT infrastructure must not be used for the following operations:

- 3.1.3.1 the downloading, storage, archiving, distribution, display, instillation etc. of, racist or pornographic images or documents, including emails, pirated or illegally copied software or data, computer viruses, worms, Trojan Horses or other malicious programs. Care should be taken in relation to emails or websites that contain jokes, pictures and political, religious or similar statements. Such sites should not be visited and such emails should not be passed on, whether internally or externally, and should preferably not be directed to the employee's or the practice's email address. It is expected that employees will inform friends and colleagues that such emails should not be sent to their work addresses, as it could constitute harassment, discrimination or intolerance and / or cause embarrassment for the employee and / or the practice.

- 3.1.3.2 deliberate or pointless damaging or overloading of computers systems or networks, the bypassing of systems protecting the privacy and data security of other users, and any other kind of deliberate damaging to the practice IT infrastructure.

3.1.4 **IMPORTANT**: The practice is always entitled to access all email accounts and all computers and / or online systems held by and for the practice. Employees should therefore ensure that information that are purely personal and confidential are not kept on the practice IT equipment (e.g. documents such as CV's, personal emails sent from the practice's email accounts even if held in the employee's name, downloads of pictures, information (e.g. houses or cars for sale) and the likes, etc.).

3.2 Data Handling:

3.2.1 When handling data and information, important rules must be followed to uphold the confidentiality of such information and compliance with all applicable laws.

3.2.2 Confidential practice information, patient / client data, practice secrets and other information only intended for internal use in the practice, must not be revealed. This includes the posting of such information on any social media sites (e.g. stating what is, at that time, happening in the practice, or something that someone did in the practice or in the hospital, etc.).

3.2.3 All restrictions in connection with copyrights, software license rights, ownership rights and other priority rights of third parties must be complied with. This means, that you are prohibited from, for example, taking practice software (such as a word-processing program) home and downloading it on your home computer.

3.3 Communications: e-mail, postings, etc.

3.3.1 Electronic communications (including e-mails and social media messages, blogs, posts at bottom of electronic media articles) leave traces that can be followed back to their source. The practice can therefore be identified as a participant. The following rules therefore apply:

- 3.3.1.1 external communications (such as with the media, social media, analysts, websites etc.) must never be in the name of the practice – if an employee is approached by the media, s / he will immediately inform the practice;

- 3.3.1.2 statements (even on Twitter / Facebook or in an email or other response to someone) which are likely to damage the practice's image or reputation must be avoided at all times. If employees are aggrieved by anything that has happened in the practice, they should use the Grievance Procedure to address this, or address it directly with the person(s) involved or responsible;

- 3.3.1.3 jokes, pictures, e-cards, photographs, e-mails with political messages or undertones, chain e-mail messages, e-mail messages that are spam (e.g. those appearing to warn of certain criminal activities, health hazards, etc.) should not be forwarded and should be deleted upon receipt. Serious instances, and where the sender is, for example, a patient or contractor of the practice, must be brought to the attention of the practice.

3.4 Mobile phones / Cellphones:

3.4.1 Where the practice has a mobile phone, such phone may also only be used for business purposes, and use includes the sending of SMS, and any other application that such phone may have (e.g. instant messaging, internet browsing, music, etc.). The mobile phone may not be removed from the practice, unless express permission is given.

3.4.2 Employees should refrain from excessive usage of their own mobile phones, and from such phones interfering with their duties in any manner whatsoever. Ring-tones should not be disturbing, offensive or rude with the context of the practice.

3.4.3 The SIM-card of a Practice mobile phone may not be removed.

3.5 Other electronic equipment:

3.5.1 Printers and photocopiers are for business purposes only.

3.5.2 In exceptional circumstances employees may, with prior permission, use the printer or photocopier for limited personal use.

3.5.3 Paper and printer cartridge usage may be monitored from time to time.

3.6 General requirements:

3.6.1 All communications, whether by phone, fax, email or otherwise, have to be professional and courteous, irrespective of whom it is directed at.

3.6.2 In cases where patients / clients or others are impatient or upset, and where the employee feels that s/he is unable to handle to situation, s/he will remain calm and polite, and request that the person speak to- or be responded to by his or her superior, at a time when the superior is available.

3.6.3 Telephone, fax, email and address lists must be kept up to date, and should be accessible to all employees and contractors at the practice, who may need them in the course of their employment.

3.6.4 Copies of all correspondence and proof of communication has to be kept, as these may be important for the business- and financial affairs of the practice, and in cases where patients, clients or others may lodge complaints or legal action. The practice may, from time to time, set criteria in terms of electronic- and hard copy filing, including the use of file names, as well as email correspondence (received and sent).

4. Discipline

4.1 Disciplinary action may be taken in cases of contravention of the Policy.

4.2 Nothing shall prevent the practice from monitoring the whole of the IT system and all communications, as outlined above.

4.3 It is expressly prohibited to utilize the internet, telephones, computers, laptops or mobile phones in infringement of this policy. The sanctions imposed by the practice may include financial compensation for damages caused and, in severe cases, dismissal after due process was followed.

4.4 The Practice will support the authorities in all justifiable criminal claims against offenders taking into account the contents of the Electronic Communications and Transactions Act 2002.