COMPUTERS EMAIL AND INTERNET POLICY

To maximise the benefits of our computer resources and minimise potential liability, employees are only permitted to use the Company's computer systems in accordance with the Company's Data Protection and Monitoring Policies and the following guidelines.

General Rules

The Company's computer systems, software and their contents belong to the company and are intended for business purposes. Employees are permitted to use the systems to assist in performing their jobs.

The Company has the right to monitor and access all aspects of its systems, including data which is stored on the Company's computer systems in compliance with the Data Protection Act 1998.

Employees must receive prior approval from management before using any part of the computer systems for personal use.

Security

The Company requires employees to log on to the Company's computer systems using their own password (where provided) which must be kept secret. Employees should select a password that is not easily broken (eg not their surnames).

Employees are not permitted to use another employee's password to log on to the computer system, where or not they have that employee's permission. If an employee logs on to the computer using another employee's password, he or she will be liable to disciplinary action up to and including summary dismissal for gross misconduct.
Any employee who disclosed his or her password to another employee will be liable to disciplinary action.

PLEASE NOTE: All employees (either in the office or caring in the field) **must not** discuss the company or company matters on any social networking sites, eg Facebook. Staff found to be ignoring this Policy will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

To safeguard the Company's computer systems from viruses, employees are not permitted to load unauthorised games or software, or to open documents or communications from unknown origins. Where the computer has internet or e-mail facilities installed, employees are not permitted to download or open files from the Internet. Before opening incoming email attachments, employees must forward them to the person responsible for IT within the office for virus checking.

The Company reserves the right to require employees to hand over all Company data held in computer useable format.

Use of Email

The Company's computer systems contain an email facility which is intended to promote effective communication within the company on matters relating to its business. Employees should only use the email system for that purpose. The Company encourages employees to make direct contact with individuals rather than communication via email.

Emails should be written in accordance with the standards of any other form of written communication, and the content and language used in the message must be consistent with best Company practice. Messages should be concise and directed to relevant individuals on a need to know basis.

Emails can be the subject of legal action, for example, claims of defamation, breach of confidentiality or breach of contract, against both the employee who sent them or the Company. Employees are also reminded that email messages may be disclosed to any person mentioned in them. Employees must therefore always be careful if they write about people in emails.

Monitoring

Monitoring will not take place unless it is carried out in accordance with the Company's Monitoring Policy. Please refer to the Company's Monitoring Policy for further details.

Inappropriate Use

Misuse of the Company's computer systems may result in disciplinary action up to and including summary dismissal. Examples of misuse include, but are not limited to the following:

- Sending, receiving, downloading, displaying or disseminating material which insults, causes offence or harasses others;
- Accessing pornographic, racist or other inappropriate or unlawful materials;
- Engaging in online chat rooms or gambling;
- Forwarding electronic chain letters or similar material;
- Downloading or disseminating copyright materials;
- Transmitting confidential information about the Company or its Services Users.
- Downloading or playing computer games; and
- Copying or downloading software.