Acceptable Usage Policy

The company makes extensive use of IT systems, for data storage, communications and as a source of information. We have adopted an IT, communications and monitoring policy in order to

- prevent inappropriate use of computer equipment (such as extended personal use or for accessing and circulating pornographic, racist, sexist or defamatory material)
- protect confidential, personal or commercially sensitive data
- prevent the introduction of viruses
- prevent the use of unlicensed software
- ensure that company property is properly looked after
- monitor the use of computer facilities to ensure compliance with internal policies and rules and to detect abuse
- IT, communication and monitoring policy

Incident Management Solutions provides access to various computing, telephone and postage facilities to allow employees to undertake the responsibilities of their position and to improve internal and external communication.

This policy sets out the company's policy on use of the facilities and it includes

- Employee responsibilities and potential liability when using the facilities
- the monitoring policies adopted by the company
- guidance on how to use the facilities

This policy has been created to

- ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring;
- protect the company and its employees from the risk of financial loss, loss of reputation or libel;
- ensure that the facilities are not used so as to cause harm or damage to any person or organisation.

This policy applies to the use of

- local, inter-office, national and international, private or public networks (including the Internet and Intranet) and all systems and services accessed through those Networks;
- desktop, portable and mobile computers and applications (including personal digital assistants (PDAs);
- mobile telephones (including the use of WAP services);
- electronic mail and messaging services.

Observation of this policy is mandatory and forms part of the Terms and Conditions of Employment. Misuse of the facilities will be treated as gross misconduct and may lead to dismissal.

Computer facilities - Use of computer systems

Subject to anything to the contrary in this policy the facilities must be used for business purposes only.

In order to maintain the confidentiality of information held on or transferred via the company's facilities, security measures are in place and must be followed at all times. A log-on ID and password is required for access to the company's network. The company reserves the right to override employee passwords and obtain access to any part of the facilities.

Employee's are responsible for keeping their password secure and should not give it to anyone, including colleagues, except as expressly authorised by the company.
Employees are expressly prohibited from using the facilities for the sending, receiving, printing or otherwise disseminating information which is the confidential information of the company or its clients other than in the normal and proper course of carrying out your duties for the company.

In order to ensure proper use of computers, employees should adhere to the following practices:

- anti-virus software must be kept running at all times
- media storage must be checked before the contents are accessed or stored on the company's network or hard drives
- obvious passwords such as birthdays and spouse names etc should be avoided (the most secure passwords are random combinations of letters and numbers)
- all files must be stored on the network drive which is backed up regularly to avoid loss of information
- always log off the network before leaving your computer for long periods of time and switch off overnight.

Software

Software piracy could expose both the company and the user to allegations of intellectual property infringement. The company are committed to following the terms of all software licences to which the company is a contracting party. This means, in particular, that

- software must not be installed onto any of the company's computers unless this has been approved in advance by a Director. They will be responsible for establishing that the appropriate licence has been obtained, that the software is virus free and compatible with the computer facilities
- software should not be removed from any computer nor should it be copied or loaded on to any computer without the prior consent of a Director.

Laptop Computers

At various times during your employment with the company, you may use a laptop. These computers, along with related equipment and software are subject to all of the company's policies and guidelines governing non-portable computers and software. However, use of a laptop creates additional problems especially in respect of potential breaches of confidentiality. When using a laptop, remember:

- you are responsible for all equipment and software until you return it. The laptop must be kept secure at all times;
- you are the only person authorised to use the equipment and software;
- you must not load or install files from any sources without first inspecting such files for viruses;
- all data kept on the laptop must be backed up regularly in order to protect data against theft or mechanical failure or corruption;
- you must password protect confidential data on external storage or on the hard drive to protect against theft;
- if you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the attention of a director;
- upon the request of the company at any time, for any reason, you will immediately return any laptop, equipment and all software to the company;
- if you are using your own laptop to connect with the company's network or to transfer data between the laptop and any of the company's computers you must ensure that you have obtained prior consent of a director, comply with their instructions and ensure that data downloaded or uploaded is free from viruses.

E-mail (Internal and External Use)

Internet e-mail is not a secure medium of communication as it can be intercepted and read. Do not use it to say anything you would not wish to be made public. If sending confidential information by e-mail, use password protected attachments.

- E-mail should be treated as any other documentation. If you would normally retain a certain document in hard copy you should retain the e-mail;
- Do not forward e-mail messages unless the original sender is aware that the message may be forwarded. If you would not have forwarded a copy of a paper memo with the same information do not forward the e-mail.
- Your e-mail inbox should be checked on a regular basis;
- As with many other records, e-mail may be subject to discovery in litigation. Like all communications, you should not say anything that might appear inappropriate or that might be misinterpreted by a reader.

Use of e-mail facilities for personal use is permitted during your lunch break providing that

- you use a separate, private e-mail address;
- such e-mails do not contain information or data that could be considered to be obscene, discriminatory, sexist, otherwise offensive and provided that such use is not part of a pyramid or chain letter;
- such e-mails are not used for the purpose of trading or carrying out any business activity other than company business.

When away from the office, you should ensure that the auto-reply service is used to inform the sender that you are unavailable. If you have any doubt as to how to use these facilities please contact your line manager.

Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, discriminatory, sexist, or otherwise offensive may constitute harassment and such use of the facilities is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

Internet

Use of the Internet, or Internet services, by unauthorised users is strictly prohibited. You are responsible for ensuring that you are the only person using your authorised Internet account and services.

Viewing, downloading, storing (including data held in RAM or cache) displaying or disseminating materials (including text and images) that could be considered to be obscene, discriminatory, sexist, or otherwise offensive may constitute harassment and such use is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

Posting information on the Internet, whether on a newsgroup, bulletin board, via a chat room or via e-mail is no different from publishing information in a newspaper. If a posting is alleged to be defamatory, libellous, or harassing, the employee making the posting and the company could face legal claims for monetary damages.

Using the Internet for the purpose of trading or carrying out any business activity other than company business is strictly prohibited.

Subject to the above you are allowed to use the Internet for personal use during your lunch break. Use of the Internet for personal use at any other time is not permitted.

For the avoidance of doubt the matters set out above include use of mobile phone text messaging, WAP, GPRS & 3,4,5G facilities.

Monitoring Policy

The policy of the company is that we may monitor use of the facilities.

The company recognises the importance of an individual's privacy but needs to balance this against the requirement to protect others and preserve the integrity and functionality of the facilities.

Principle reasons for this are to

- detect any harassment or inappropriate behaviour by employees, ensuring compliance with contracts of employment and relevant policies including the health and safety, ethical and sex discrimination policies
- ensure compliance of this policy
- detect and enforce the integrity of the facilities and any sensitive or confidential information belonging to or under the control of the company
- ensure compliance by users of the facilities with all applicable laws (including Data Protection), regulations and guidelines published and in force from time to time
- monitor and protect the well-being of employees.
- Making service improvements in quality.

The company may adopt at any time a number of methods to monitor use of the facilities. These may include

- recording and logging of internal, inter-office and external telephone calls made or received by employees using its telephone network (including where possible mobile telephones). Such recording may include details of length, date and content;
- recording and logging the activities by individual users of the facilities. This may include opening e-mails and their attachments, monitoring Internet usage including time spent on the Internet and web sites visited;
- physical inspections of individual users' computers, software and telephone messaging services;
- periodic monitoring of the facilities through third party software including real time inspections;
- physical inspection of an individual's post
- archiving of any information obtained from the above including e-mails, telephone call logs and Internet downloads.

The company will not (unless required by law)

- allow third parties to monitor the facilities; or
- disclose information obtained by such monitoring of the facilities to third parties.

The company may be prohibited by law from notifying employees using the facilities of a disclosure to third parties.

General Guidance

Never leave any equipment or data (including client files, laptops, computer equipment, mobile phones and PDAs) unattended on public transport or in an unattended vehicle.

When using e-mail or sending any form of written correspondence

- use only authorised Incident Management Solutions e-mail templates;
- do not use manufacturer's logo's, signs or symbols of accreditation without prior permission from a director;
- do not use foul or abusive language, text speak, slang or other familiarities;
- be careful what you write. Never forget that e-mail and written correspondence are not the same as conversation. They are a written record and can be duplicated at will
- use normal capitalisation and punctuation. Typing a message all in capital letters is the equivalent of shouting at the reader;
- check grammar and spelling;
- do not forget that e-mails and other forms of correspondence should maintain the high standards expected by the company. Where applicable, use formal headings and introductions such as "Dear ..." and "Yours sincerely" etc.

Observation of this Policy is mandatory and forms part of the Terms and Conditions of Employment. Misuse of the facilities will be treated as gross misconduct and may lead to dismissal.