Safeguards

A) RIGHTS OF SEARCH

1) Although we do not have the contractual right to carry out searches of employees and their property (including vehicles) whilst they are on our premises or business, we would ask all employees to assist us in this matter should we feel that such a search is necessary.

2) Where practicable, searches will be carried out in the presence of a colleague of your choice who is available on the premises at the time of the search. This will also apply at the time that any further questioning takes place.

3) We reserve the right to call in the police at any stage.

B) CONFIDENTIALITY

1) All information that:

   a) is or has been acquired by you during, or in the course of your employment, or has otherwise been acquired by you in confidence;

   b) relates particularly to our business, or that of other persons or bodies with whom we have dealings of any sort; and

   c) has not been made public by, or with our authority;

   shall be confidential, and (save in the course of our business or as required by law) you shall not at any time, whether before or after the termination of your employment, disclose such information to any person without our prior written consent.

2) You are to exercise reasonable care to keep safe all documentary or other material containing confidential information, and shall at the time of termination of your employment with us, or at any other time upon demand, return to us any such material in your possession.

3) You must make yourself aware of our policies on data protection in relation to personal data and ensure compliance with them at all times.

C) COMPANY PROPERTY AND COPYRIGHT

All written material, whether held on paper, electronically or magnetically which was made or acquired by you during the course of your employment with us, is our property and, where appropriate, our copyright. At the time of termination of your employment with us, or at any other time upon demand, you shall return to us any such material in your possession.

D) STATEMENTS TO THE MEDIA

Any statements to reporters from newspapers, radio, television, etc. in relation to our business will be given only by the Managing Director.

E) DATA PROTECTION

The General Data Protection Regulation (GDPR) and the current Data Protection Act regulate our use of your personal data. As an employer it is our responsibility to ensure that the personal data we process in relation to you is done so in accordance with the required principles. Any data held shall be processed fairly and lawfully and in accordance with the rights of data subjects.
We will process data in line with our privacy notices in relation to both job applicants and employees.

You have several rights in relation to your data. More information about these rights is available in our "Policy on your rights in relation to your data". We commit to ensuring that your rights are upheld in accordance with the law and have appropriate mechanisms for dealing with such.

We may ask for your consent for processing certain types of personal data. In these circumstances, you will be fully informed as to the personal data we wish to process and the reason for the processing. You may choose to provide or withhold your consent. Once consent is provided, you are able to withdraw consent at any time.

You are required to comply with all company policies and procedures in relation to processing data. Failure to do so may result in disciplinary action up to and including dismissal.

F) INVENTIONS/DISCOVERIES

An invention or discovery made by you will normally belong to you. However, an invention or discovery made by you will become our property if it was made:

a) in the course of your normal duties under such circumstances that an invention might reasonably be expected to result from those duties;

b) outside the course of your normal duties, but during duties specifically assigned to you, when an invention might reasonably be expected to result from these; and

c) during the course of any of your duties, and at the time you had a special obligation to further our interests arising from the nature of those duties, and your particular responsibilities.

G) VIRUS PROTECTION PROCEDURES

In order to prevent the introduction of virus contamination into the software system the following must be observed:

a) unauthorised software including public domain software, USBs, external hard drives, CDs or internet downloads must not be used; and

b) all software must be virus checked using standard testing procedures before being used.

H) USE OF COMPUTER EQUIPMENT

In order to control the use of the Company's computer equipment and reduce the risk of contamination the following will apply:

a) the introduction of new software must first of all be checked and authorised by the Operations Director and/or Office Manager before general use will be permitted;

b) only authorised staff should have access to the Company's computer equipment;

c) only authorised software may be used on any of the Company's computer equipment;

d) only software that is used for business applications may be used;

e) no software may be brought onto or taken from the Company's premises without prior authorisation;

f) unauthorised access to the computer facility will result in disciplinary action; and

g) unauthorised copying and/or removal of computer equipment/software will result in disciplinary action, such actions could lead to dismissal.

I) E-MAIL AND INTERNET POLICY

1) Introduction

The purpose of the Internet and E-mail policy is to provide a framework to ensure that there is continuity of procedures in the usage of internet and e-mail within the Company. The internet and e-mail system have established themselves as an important communications facility within the Company and have provided us with contact with professional and academic sources throughout the world. Therefore, to ensure that we are able to utilise the system to its optimum we have devised a policy that provides maximum use of the facility whilst ensuring compliance with the legislation throughout.

2) Internet

Where appropriate, duly authorised staff are encouraged to make use of the Internet as part of their official and professional activities. Attention must be paid to ensuring that published information has relevance to normal professional activities before material is released in the Company name. Where personal views are expressed a disclaimer stating that this is the case should be clearly added to all correspondence. The intellectual property right and copyright must not be compromised when publishing on the Internet. The availability and variety of information on the Internet has meant that it can be used to obtain material reasonably considered to be offensive. The use of the Internet to access and/or distribute any kind of offensive material, or material that is not work-related, leaves an individual liable to disciplinary action which could lead to dismissal.

3) Procedures – Acceptable/Unacceptable Use

a) unauthorised or inappropriate use of the internet system may result in disciplinary action which could result in summary dismissal.

b) the internet system is available for legitimate business use and matters concerned directly with the job being done. Employees using the internet system should give particular attention to the following points:

i) comply with all of our internet standards;

ii) access during working hours should be for business use only;

iii) private use of the internet should be used outside of your normal working hours.

c) the Company will not tolerate the use of the Internet system for unofficial or inappropriate purposes, including:

i) accessing websites which put our internet at risk of (including but not limited to) viruses, compromising our copyright or intellectual property rights;

ii) non-compliance of our social networking policy;

iii) connecting, posting or downloading any information unrelated to their employment and in particular pornographic or other offensive material;

iv) engaging in computer hacking and other related activities, or attempting to disable or compromise security of information contained on the Company's computers.

You are reminded that such activities (iii. and iv.) may constitute a criminal offence.

4) E-mail

The use of the e-mail system is encouraged as its appropriate use facilitates efficiency. Used correctly it is a facility that is of assistance to employees. Inappropriate use however causes many problems including distractions, time wasting and legal claims. The procedure sets out the Company's position on the correct use of the e-mail system.

5) Procedures - Authorised Use

a) unauthorised or inappropriate use of the e-mail system may result in disciplinary action which could include summary dismissal.

b) the e-mail system is available for communication and matters directly concerned with the legitimate business of the Company. Employees using the e-mail system should give particular attention to the following points:

i) all comply with Company communication standards;

ii) e-mail messages and copies should only be sent to those for whom they are particularly relevant;

iii) e-mail should not be used as a substitute for face-to-face communication or telephone contact. Abusive e-mails must not be sent. Hasty messages sent without proper consideration can cause upset, concern or misunderstanding;

iv) if the e-mail is confidential the user must ensure that the necessary steps are taken to protect confidentiality. The Company will be liable for infringing copyright or any defamatory information that is circulated either within the Company or to external users of the system; and

v) offers or contracts transmitted by e-mail are as legally binding on the Company as those sent on paper.

c) The Company will not tolerate the use of the e-mail system for unofficial or inappropriate purposes, including:

i) any messages that could constitute bullying, harassment or other detriment;

ii) personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters);

iii) on-line gambling;

iv) accessing or transmitting pornography;

v) transmitting copyright information and/or any software available to the user; or

vi) posting confidential information about other employees, the Company or its clients or suppliers.

6) Monitoring

We reserve the right to monitor all e-mail/internet activity by you for the purposes of ensuring compliance with our policies and procedures and of ensuring compliance with the relevant regulatory requirements. This includes monitoring of any additional accounts you may be requested to set up for the purposes of performing your work tasks, which are subject to the same rules as your work email account. Information acquired through such monitoring may be used as evidence in disciplinary proceedings. Monitoring your usage will mean processing your personal data. You may read more about the data we hold on you, why we hold it and the lawful basis that applies in the employee privacy notice.

J) USE OF SOCIAL NETWORKING SITES

Social media can be a very powerful tool which enhances the services we provide to our clients. We use social media to advertise any on-going promotions, products and other relevant information. Only authorised employees should use our Company sites and a professional, positive approach should be maintained at all times.

Employees should be aware of crossing the professional boundaries and hence are not permitted to make or accept "friend requests" to/from our clients on their private social media accounts.

Any work related issues or material that could identify an individual who is a client or work colleague, which could adversely affect the Company a client or our relationship with any client must not be placed on your private social network accounts. For the avoidance of doubt work related matters must not be submitted on any such site at any time either during or outside of working hours.

K) KEYHOLDING/ALARM SETTING

If you are an allocated key holder, you must ensure that all procedures and guidelines are followed when securing the building prior to leaving. The keys and any security measure such as alarm codes must be kept safe at all times. You must not give the keys or alarm code to any third party unless authorisation is obtained from the Operations Director and/or Office Manager. Any loss or damage caused as a result of your failure to follow procedures or your negligence in ensuring the safekeeping of the keys and alarm code will result in disciplinary action which could lead to your summary dismissal. We also reserve the right to deduct the cost of any loss, repair or replacement from any monies owing to you.

Any breaches or security issues including the loss or theft of keys must be reported immediately to the Operations Director and/or Office Manager.

To satisfy the requirements of our insurers and to protect us from fire and theft, you must secure all properties and premises when unattended. The last person to leave the premises must ensure lights and appropriate electrical equipment are switched off, windows and doors are secure and alarms are set accordingly.

L) CASH HANDLING

1) On the occasion you are handling cash, you must do so accurately.

2) Any discrepancies must be reported immediately to the Operations Director and/or Office Manager.

3) You must return all monies to the office promptly.

4) All notes should be checked for forgeries. Where a forgery is identified, please notify the Operations Director and/or Office Manager.

5) All monies must be stored appropriately.

M) CLOSED CIRCUIT TELEVISION

Closed circuit television cameras are used on our premises for security purposes. We reserve the right to use any evidence obtained in this manner in any disciplinary issue. We will ensure all personal data obtained in this way is processed in line with the current Data Protection Act. You may refer to the employee privacy notice for more information on the data we hold, the reasons we hold it and the lawful basis which applies.