Computer and Telephone Use Policy

Computer use

You may have access to computers at work for use in connection with the Company's business. Computers are provided to undertake business-related activities only. If you are discovered unreasonably using the Company's computers for personal and private purposes, disciplinary action will be taken under the Company's disciplinary procedure. Vandalism of, or otherwise intentionally interfering with, the Company's computers or network constitutes a potential gross misconduct offence and could result in your summary dismissal.

Security

As many computer files contain confidential or sensitive business information, the Company takes the security of these files very seriously. You are therefore required to comply with the following basic security precautions:

- If you need to leave your computer for more than a couple of minutes, lock the computer screen.
- If you need to leave your computer for a long period of time, log off. Never leave an unattended computer logged on
- When creating a computer password, do not use one that is obvious, such as your date of birth or the name of a close family member. Passwords should preferably be a mix of letters and numbers and should not be the same as any other personal passwords you may have (such as internet banking passwords)
- Always keep your password private, do not write it down and do not divulge it to anyone else.
- If you suspect that someone knows your password, change it.
- Change your password at regular intervals in any event.
- Always shut down your computer when you go home at the end of your working day.
- If you notice any suspicious activity, for example an employee trying to gain unauthorised access to another member of staff's computer, notify your line manager immediately.

Data

The computers and the data they contain are provided to undertake business-related activities and to enable you to carry out your job duties. As such, data should not be amended, deleted, copied or taken away unless this is both specifically related to the work you are undertaking and you have the authority to make such amendment, deletion or copy. In particular, you should not delete or amend any documentation or programs which are stored on the Company's communal drives unless you have the requisite level of authority to do so.

Non-work related data should not be copied onto or stored on Company computers.

Computer software, games and viruses

The Company licences the use of computer software from a variety of outside companies. The Company does not own this software and, unless authorised by the software developer, neither the Company nor any of our employees have the right to reproduce it. To do so constitutes an infringement of copyright. Contravention is a disciplinary matter and will be dealt with under the Company's disciplinary procedure.

Software that you need to use to carry out your job duties will be provided and installed on your computer for you. Installation of any non-approved software is prohibited. This includes screen savers and wallpapers. Only the IT Department have the authority to load new software onto your computer. Even then, software may be loaded only after having been checked for viruses. If you contravene this, you will face disciplinary action under the Company's disciplinary procedure.

The Company's computer network makes it vulnerable to viruses. All work computers have virus protection software installed. You must not re-configure or disable this software. If you suspect your computer may

have become infected with a virus, turn it off immediately and contact the IT Department.

You may only access any computer games that are on the network outside your normal working hours. You must not install your own games on your work computer.

Use of portable storage devices

You may be provided with portable storage devices, such as memory sticks and portable hard drives, that can be plugged into the USB port of a computer. Whilst they are provided so as to allow for the copying and transferring of files and images between your desktop or laptop computer, their small size and storage capacity makes them vulnerable to misuse. For this reason, if you are issued with one of these devices, you must not transfer any data to a third party computer (including one at home) without first having obtained approval from the IT Department. If you transfer files to a third party without permission, you may be subject to disciplinary action. In the event that this involves the deliberate transfer of sensitive commercial information to a competitor, it will be treated as gross misconduct and could result in your summary dismissal.

E-mail and internet use

You may also have access to e-mail and the internet for use in connection with the Company's business and as part of the normal execution of your job duties. The purpose of these rules is to protect the Company's legal interests. Unregulated access increases the risk of you inadvertently forming contracts through e-mail and increases the opportunity for wrongful disclosure of confidential information. In addition, carelessly worded e-mail can expose the Company to an action for libel. As such, e-mail to clients, customers and suppliers must follow the Company's designated house style, which will be supplied to you. Failure to follow house style is a disciplinary matter and will be dealt with under the Company's disciplinary procedure. E-mail should not be used for unsolicited correspondence or marketing campaigns and you must not commit the Company financially by e-mail unless you have been granted a specific level of delegated authority to do so.

You are only permitted to surf the internet for personal and private use, log on to social networking and video sharing websites such as Facebook, MySpace, Bebo, Twitter and YouTube or use the Company IT systems to keep a personal weblog ('blog') at designated times during the day. The designated times are either before or after your normal working hours and during your lunch break. The Company nevertheless reserves the right to restrict access to social networking and video sharing websites at any time. The Company considers personal use of the internet to include activities such as personal online shopping, booking holidays and banking. You must not use your work e-mail address to place orders online for personal goods and services.

Further, you are not permitted to spend excessive time 'chatting' by e-mail for personal and private purposes during your normal working hours. You are also prohibited from using e-mail to circulate any non-business material. Excessive time spent online leads to loss of productivity and constitutes an unauthorised use of the Company's time. You must not send offensive remarks, jokes, pictures or videos by e-mail, via social networking websites or blogs which are capable of amounting to harassment because of age, disability, gender reassignment, race (including colour, nationality and ethnic or national origins), religion or belief, sex and/or sexual orientation under the section on **Equal Opportunities and Dignity at Work**. You are also prohibited from using the Company's electronic communications as a means of intimidating or bullying employees or third parties.

A breach of these rules is a disciplinary offence and will be dealt with in accordance with the Company's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in your summary dismissal.

Logging on to sexually explicit websites or the downloading and/or circulation of pornography or other grossly offensive, illegal or obscene material or using the internet for gambling or illegal activities constitutes gross misconduct and could result in your summary dismissal under the Company's disciplinary procedure. Be aware that 'rogue' websites exist that appear harmless but instead direct you automatically to another website that may contain inappropriate material. If this happens, please contact the IT Department immediately.

Use of instant messaging systems must be approved in advance by the IT Department.

Social networking and video sharing websites

When logging on to and using social networking and video sharing websites and blogs at any time, you must not:

- Publicly identify yourself as working for the Company, make reference to the Company or provide information from which others can ascertain the name of the Company.
- Conduct yourself in a way that is detrimental to the Company or brings the Company into disrepute.
- Use your work e-mail address when registering on such sites.
- Allow your interaction on these websites or blogs to damage working relationships between employees and clients of the Company.
- Include personal information about the Company's employees, suppliers, customers or clients without their express consent (you may still breach this even if employees, suppliers, customers or clients are not expressly named in the websites or blogs as long as the Company reasonably believes they are identifiable).
- Make any derogatory, offensive or defamatory comments about the Company, its employees, suppliers, customers or clients (you may still breach this even if the Company, its employees, suppliers, customers or clients are not expressly named in the websites or blogs as long as the Company reasonably believes they are identifiable).
- Make any comments about the Company's employees that could constitute unlawful discrimination, harassment or bullying.
- Disclose any confidential information belonging to the Company or our suppliers, customers or clients or any information which could be used by a competitor.

If you are discovered contravening these rules, you may face serious disciplinary action under the Company's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in your summary dismissal. The Company also reserves the right to deny, remove or limit e-mail and/or internet access to or from you if you contravene these provisions.

Downloading information from the internet and file sharing

You must not use work computers to make illegal downloads of material that is subject to copyright. This includes, but is not limited to, music, film and business software. Downloading and any subsequent file sharing of this material constitutes an infringement of copyright. This also applies to any download or dissemination of material made outside of your normal working hours. Any breach is likely to lead to disciplinary action being taken.

You may need to download documents and information from the internet in order to undertake your job duties. You should only download documents and information that you are sure about and which you require to fulfill your job duties. With the rapid spread of computer viruses via the internet, you must take care when accessing websites that you are not familiar with or when downloading documents or information.

You must not download any programs from the internet without the prior approval of the IT Department. Some websites require additional add-in software to display the page completely. These add-ins usually provide additional sound or visual effects. Under no circumstances should these be downloaded without the prior approval of the IT Department.

E-mail and internet monitoring

The Company reserves the right to monitor your internal and external e-mails and use of the internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes for such monitoring are:

- To promote productivity and efficiency.
- To ensure the security of the system and its effective operation.
- To ensure there is no unauthorised use of the Company's time, for example to check that you have not been using e-mail to send or receive an excessive number of personal communications.

- To ensure the smooth running of the business if you are absent for any reason and communications need to be checked.
- To ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to unlawful harassment.
- To ensure that inappropriate websites are not being accessed.
- To ensure there is no breach of commercial confidentiality.

Communications of a sensitive or confidential nature should not be sent by e-mail because it is not guaranteed to be private. When monitoring e-mails, the Company will, save in exceptional circumstances, confine ourselves to looking at the address and heading of the e-mails. However, where circumstances warrant it, the Company may open e-mails and access the content. In this case, we will avoid, if possible, opening e-mails clearly marked as private or personal.

Reading and storing e-mails

You must check your mailbox regularly during your normal working hours. It is your responsibility to read and action any e-mail you receive.

The e-mail system is not to be used as a storage area. Unwanted messages should be deleted completely. Important information or files should be saved into your private or communal data areas or into e-mail folders.

If you are going to be out of the office for a day or longer and as such you will be unable to check your e-mail, you should switch on your 'out of office assistant' message. E-mail received in your absence will not normally be read by other members of staff unless you have specifically requested a colleague to undertake this task. However, e-mail may need to be checked by your line manager for business-related reasons when you are absent for any reason. It may therefore be unavoidable that some personal e-mails might be read in these circumstances.

E-mail viruses and spam

All incoming and outgoing external e-mails are checked for computer viruses and, if a virus is found, the message will be blocked. E-mails may also be checked for other criteria, for example, having an attached image file or containing offensive or inappropriate material or including a 'banned' word or from a 'banned' user under the criteria in the Company's spam software which indicates the message is spam. Again, the e-mail will be blocked. The Company reserves the right to block and then read these messages to ascertain whether they are business-related.

If you receive an e-mail or data file that is in a format or comes from a source that you do not recognise, do not open the item but contact the IT Department immediately. Any executable files received by e-mail must be referred to the IT Department for clearance before any other action is taken.

If you receive any unsolicited e-mails or spam that manages to bypass the Company's spam software, you must not respond in any way. Please forward the e-mail to the IT Department and they will add the sender to the list of banned users. Some spam e-mails may offer the option to opt out of receiving them. Be aware that this is sometimes used as a way by unscrupulous spammers of validating a live e-mail address.

Telephone use

The Company's telephone lines (including Company mobile phones) are for your exclusive use in connection with the Company's business. Whilst the Company will tolerate essential personal telephone calls concerning your domestic arrangements, excessive use of the telephone for personal calls is prohibited. This includes lengthy, casual chats and calls at premium rates. Not only does excessive time engaged on personal telephone calls lead to loss of productivity, it also constitutes an unauthorised use of the Company's time. If the Company discovers that the telephone has been used excessively for personal calls, this will be dealt with under the Company's disciplinary procedure and you will also be required to pay to the Company the cost of personal calls made.

Acceptable telephone use should be no more than five minutes of personal calls in each working day. Personal telephone calls should be timed so as to cause minimum disruption to your work and should, as a general rule, only be made during breaks except in the case of a genuine emergency.

Telephone monitoring

You should be aware that telephone calls made and received on the Company's telephone network will routinely be monitored and recorded to assess your performance, to ensure client and customer satisfaction and to check that the use of the telephone system is not being abused or used in an unauthorised manner. In addition, an itemised call log may be maintained and retained of all calls made and received on the Company's telephone network. This may include details of the external caller's number and the date, time and duration of the call.

Your voicemail messages may be checked by your line manager for business calls when you are absent for any reason. It may therefore be unavoidable that some personal messages might be heard in these circumstances.

If you wish to make or take a particularly sensitive, private or confidential personal telephone call, you are advised that there is a designated telephone available, which will not be subject to any form of monitoring or recording by the Company. For further details, please contact the HR Department.

Mobile phones

Whilst the Company will tolerate the use of your own mobile phone for essential personal calls during your normal working hours, excessive use for personal calls is prohibited. Also prohibited are lengthy calls, casual chats, text messaging, e-mailing, web browsing and the taking of video and/or still images. Your mobile phone should be set to a silent ring during your normal working hours. If you wish to use your mobile phone, you should do so outside your normal working hours or during your lunch break.