COMPUTER POLICY

Computer usage

Some employees have access to computers at work for use in connection with the Company’s business. Computers are provided to employees to undertake business-related activities only. Employees who are discovered unreasonably using the Company’s computers for personal and private purposes will be dealt with under the Company’s disciplinary procedure.

Vandalism of, or otherwise intentionally interfering with, the Company’s computers/network constitutes a gross misconduct offence and could render the employee liable to summary dismissal.

Security

As many computer files contain some form of confidential or otherwise sensitive business information, the Company takes the security of these files very seriously. With this in mind, we have introduced some basic security precautions that all employees must abide by.

These are as follows:

• 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

• computer passwords are considered our confidential information even if you are using your personal password for social networking to login to our work systems. 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 (including other members of staff), except for ……… *(insert details)*

• if you suspect that someone knows your password, change it in the normal way

• change your password at regular intervals in any event

• always shut down your computer when you go home at the end of the 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 manager immediately

• if you are provided with a Company computer for use in your home, family members [are/are not] (amend as necessary) allowed to use it

• (insert any other measures).

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.

Use of portable storage devices

Some employees may be provided with portable storage devices, such as memory sticks and portable hard drives, which 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 an employee’s desktop or laptop computer, their small size and storage capacity makes them vulnerable to misuse. For this reason, any employee issued with these devices must not transfer any data to a third party computer (including one at home) without first having obtained approval from their manager. From time to time, user guidelines will be produced on the usage of such devices and employees will be expected to follow them. Any employee who transfers files to a third party without permission is likely to 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.

Software

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 its 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 in accordance with 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 has the authority to load new software onto the network system. Even then, software may be loaded only after having been checked for viruses.

Viruses

The Company’s computer network makes it vulnerable to viruses. All Company computers have virus protection software installed. Re-configuring or disabling this software is prohibited.

If your computer starts to behave strangely or you suspect it may have become infected with a virus, turn it off immediately and contact the IT department.

***Games***

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

Remote access

Some employees may spend at least part of their working week on Company business away from the premises. This includes sales staff, .......... *(insert other categories as applicable)* and those who may work from home. These employees and any others who may work remotely on an informal basis should be aware that all aspects of this policy apply equally to them. Remote working employees will also be expected to comply with any additional guidelines that may be introduced in order to reduce the likelihood of the Company’s computer networks being compromised as a result of remote access.

Employees must not allow any family members or other third parties to either use the company’s computer equipment (including software) or to access or view its internal IT networks.

Temporary workers

From time to time, the Company may need to use temporary staff in order to cover busy periods or annual leave. Should any temporary worker need to use a computer as part of their job role, the manager responsible for their day-to-day supervision will be required to bring this policy and its contents to their attention.

It is also Company policy that any temporary workers who are required to use a computer for more than ....... *(insert number)* days will be given their own log-in details. Managers will need to identify if there are any directories or computer files on the computer that will be used by the temporary worker that are of a sensitive or confidential nature. If so, the IT department will need to be involved in restricting access to them. The same principles apply to any self-employed contractors engaged by the Company.

Managers’ duties

Managers will be required to notify the IT department in advance of any computer users that will be leaving the Company. This should be done at least ....... *(insert period)* before the employee leaves, so that the individual’s account can be closed down on their departure.

Likewise, managers should notify the IT department in advance of any new computer users that will be starting work for the Company. This should be done at least ....... *(insert period)* before the employee starts, so that the individual’s account can be set up ready for their start date.

From time to time, the Company will review its storage of confidential information and the media upon which it is stored. Managers will be expected to co-operate in terms of identifying such files, the employees or other staff with access to them and the file locations.

Contravention of this policy

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under the Company’s disciplinary procedure.