

## **COMPUTER, E-MAIL & INTERNET POLICY**

### **USE OF COMPUTERS, E-MAIL AND INTERNET**

The Company's policy on the use of computers, e-mail (including any mobile devices) and the internet, is designed to protect both the Company and individuals against misuse and to provide guidelines to users about the appropriate use of these systems.

The computer systems used by [Company] are essential to the Company's operations. You should ensure that, at all times, your actions or in-actions do not compromise the working operation of the computer system. If you are unclear about any aspect of the policy you should speak to your Manager or the person responsible for the computer system. Any breach of the policy on the use of computers, e-mail and the internet, will be dealt with through the Disciplinary Procedure.

### **SECURITY OF THE COMPUTER SYSTEM**

In order to avoid unnecessary degrading of the network performance and to protect the network from viruses, under no circumstances may unauthorised software, programs or data be loaded (or downloaded from the internet) onto the computer system or your own workstation.

Under no circumstances may illegal, defamatory, inappropriate or offensive software or material be accessed, installed, stored or downloaded onto any computer/workstation. In the event of any such software or material being found, you will be personally liable. This liability may include criminal prosecution, fines or penalties. In addition, such action is considered to be gross misconduct and the individuals concerned will be subject to the Disciplinary Procedure.

Copies of programs or data must not be taken or removed from the Company's premises without the express permission of a Director (if authorised by the Data Owner). [Company] regards computer system security to be of paramount importance. Any individual action or inaction that compromises this security is considered to be a serious matter. Detailed below are guidelines regarding use of the computers:

- If you experience a problem with your computer you should inform your Manager or the person responsible for the computer system as soon as the problem arises. You should write down the details of any error messages so these can be communicated to the person who will deal with the problem;
- You may only log-on to the network using your own account and you should keep your password confidential.

### **THE INTERNET**

[Company] authorises certain individuals to access the internet, or parts of the internet, for the performance of their duties. Private use of the internet is acceptable provided you have gained the prior permission of your Manager and do this outside of working hours. [Company] will investigate cases where individual employees spend excessive amounts of their time on the internet.

The Company reserves the right to further investigate the use of the internet by individual employees or indeed all employees, where it believes there is a breach of the Company's internet Policy or to protect the rights of other employees.

You should not deliberately access sites that may contain material that is (or may be) illegal, defamatory, or have content that is pornographic, inappropriate or offensive and, under no circumstances whatsoever, should such material be downloaded or distributed within the Company.

Any unauthorised use of the internet will be treated as a disciplinary matter. In particular, you should be aware that the Company will treat any downloaded material that may be regarded as harassment or discrimination as a serious disciplinary matter. Detailed below are further guidelines regarding the internet:

- You may not access any IRC or ICQ type services using the Company's computer systems (e.g. chat rooms);
- You may not use the Company's internet facilities for personal financial or commercial gain.

## **USE OF SOCIAL NETWORKING WEBSITES**

The Company reserves the right to monitor access to social networking websites such as, but not limited to FaceBook, My Space, You Tube, personal blogs or any blogs whatsoever or any such sites. Should the Company feel that usage of such items is excessive; your access to the internet or to such sites may be restricted or withdrawn. Should further usage occur breaching such penalties, then this will be considered by the Company as a disciplinary matter.

You must not make comments or down/upload material to such sites that may be inappropriate, offensive or bring the Company into disrepute. Such behaviour will be considered to be gross misconduct.

## **USE OF E-MAIL**

Although e-mail communication is in common use, it can have legal implications for the people that use it and the Company for which you work. In particular, you should be aware that the contents of e-mails sent from a Company's computer system can bind the Company contractually or can give rise to defamation claims.

Detailed below are guidelines on the use of e-mail with [Company]:

- The provision of e-mail on the computer system is generally for business use. Private e-mails outside [Company] are allowed provided you have gained the prior permission of your Manager and read / respond to them outside of working hours;
- Do not write anything in an e-mail that you would not put in a letter or say to a person's face. You should not use obscene, vulgar, abusive or inappropriate language, pornographic or offensive pictures or other such material in e-mails;
- Be aware that e-mails could possibly have a contractual implication or become legally binding;
- Do not send multiple or chain e-mails;
- Do not forward e-mails to colleagues inside [Company] unless they are business-related;
- Do not post your personal details or the details of [Company] to an internet web site;
- Report all unsolicited e-mail that is received to your Manager or the person responsible for the computer system.

You should be aware that [Company], via its ISP, monitors all e-mail activity. The Company also reserves the right to investigate the e-mail activity of individual employees, where there are reasonable grounds to believe that the Company's e-mail policy has been breached, to protect the rights of other employees or to investigate internal or external complaints about malicious e-mails.

It may be necessary to access the incoming e-mails of individual employees during their absence. This would normally apply to employees who have regular contact with customers or suppliers, and where the Company has identified the need for this relationship to be actively managed in the absence of the employee. There may also be other occasions where, for business reasons, the Company needs to access e-mails in order to retrieve information. Therefore, you are advised not to include personal or private information in e-mails that are sent or received via the Company's computer system.

You should note that [Company] provides a facility to delete personal e-mails from your own computer. The Company recommends that you regularly review any personal e-mails that are stored in your Inbox, and delete them from your computer. If you are unsure of how to delete unwanted e-mails, you should contact your Manager or the person responsible for the computer system.