COMPUTER USAGE POLICY

POLICY

While the internet is a great resource for our organisation, it is the responsibility of each employee to use this resource responsibly and respectfully. Company computers are provided for work related use. These computers should not be used for personal use without prior approval from your supervisor or manager.

GUIDELINES

Where personal use is permitted, it is assumed that the predominant use of these resources will be work related, and that any personal use of electronic mail or the internet will be limited; never a priority over work matters. If an employee is found spending excessive time on personal use of these resources, this privilege may be revoked for that employee.

You are not permitted to install your own software on any company computers, without prior approval from your supervisor or manager. Failure to comply may result in users being held personally responsible for any data loss or penalties imposed for breach of copyright.

You may not use company email to harass, send abusive email, defame or disclose unauthorised information or transmit pornography. You should not participate in chain emails, and should not view any non work related graphics which you receive. You may not use email to forward encrypted confidential or propriety information. Employees may encrypt their email and files only with the use of software approved by the company. This software may provide for retention by the company of any key necessary to access encrypted messages. You must scan any executable files received via the internet with an updated virus checker. Improper usage of email may pose a threat to system security, the privacy of staff and others, and the legal liability of the company.

You may not use the web to view pornographic material. Unless permission has been granted for personal use, you may not use the web to browse non work related sites. You should not download any unauthorised software from the internet. Failure to comply may result in the termination of your employment.

You are required to provide a secure password for use on the company's computer network. Messages cannot be protected from unauthorised access if caused by users failing to maintain password confidentiality, or leaving the computer unattended when he or she has logged onto the system. Users will be responsible for any email sent using their unique log in and password, or for any web sites visited while logged in. Users are encouraged to use password screensavers to avoid unauthorised use of their computer.

USB Pens or Flash Drives may only be used if written approval has been granted for their use. Approval will be granted on a case by case basis. Any approval will clearly state the reason for their use, and the data that may be stored on these drives. You may be required to encrypt the data stored on your USB Pen or Flash Drive.

You may not use CD Burners or any other form of data storage to transport company information without prior written permission. If permission is granted, it may be a requirement that any data is stored in encrypted format.

Sensitive information stored on laptop computers must be encrypted. This ensures that the date remains confidential if the computer is lost of stolen. You may not copy any information or software stored on your desktop or laptop computer for personal use.

Failure to comply with any of the above requirements may result in disciplinary action being taken, which may lead to the termination of your employment.

What is Confidentiality and Sensitive Information?

Company and/or sensitive information includes and will include all trade and business secrets and other confidential information and documents relating to the affairs or business of the Company or any other person with whom you come into contact as a result of your employment with the Company or may come into your possession in the course and by reason of your employment whether or not the same were originally supplied by the Company.

Confidential information includes any information (written or verbal) of a commercial, technical or financial type which is not publicly available.

You must not make unauthorised copies of any material (original or not) such as correspondence, company manuals, computer printouts, floppy discs, customer lists, rate schedules, diaries, file notes or any other material whether or not compiled or made by you, or to which you have access as part of your employment.

All such material is and remains the property of the Company. All Company property must be returned on termination of your employment.

EMAIL

Electronic mail sent from the Company should be treated the same any other communication that is sent. All communications represent the company as a whole, and as such, should be written in a professional and appropriate manner. This also applies to any material that is published on the internet.

Although network security features have been implemented, your email can still be accessed, and your internet activity can still be monitored by the Company. Email should be regarded as an insecure medium unless it has been encoded or encrypted. Email is often compared to a postcard in that anyone who receives it can read it. Email may also be read if it is stored on a server during transmission. System administrators are also capable of reading the contents to all emails sent and by the Company network. This means that the Company has access to all emails sent or received over the internet or intranet.

Most electronic documents are backed up and therefore recoverable. In other words, once you delete your email from your inbox it may still be recoverable. Other information stored on the network includes the date and time the email was sent or received, as well as the email address of the sender and recipients.

The Company reserves the right to view any email on its server or any email that has been backed up at any time. The Company will not view email logs unless there is a legitimate cause to do so. Audit information will not be released to a third party without the production of a legal authority. Where the Company initiates action to actively monitor a persons email, that person will be informed in writing that this action will occur, and be provided a reason for this action.

You should be aware that failure to comply with this policy may result in disciplinary procedures, which may lead to the termination of your employment.