Employees are responsible for maintaining the security of their computer equipment and software and where employees have access to confidential information they must ensure that it remains secure:

* You should not use the Company’s computers unless you are competent to do so and should ask for training if you need it.
* You must not introduce or operate any programs or data (including computer games) or open suspicious e-mails which have not first been checked by the Company for viruses.
* You should not let anyone else know your password. If you believe that someone knows your password you must change it immediately.
* The internet facility is provided for Company related activities only. Use of the internet during working hours for personal reason is prohibited.
* Downloading of any program or file which is not specifically related to your job is strictly prohibited.
* Viewing, retrieving or downloading of pornographic material, or any other material which the Company believes is unsuitable, at any time, is strictly prohibited and constitutes gross misconduct.
* Any e-mail message which is abusive, discriminatory on grounds of race, sex or disability, or defamatory is not permitted and constitutes gross misconduct.
* Personal data should be obtained only for the purpose specified and should be adequate, relevant and not excessive for the purposes required.
* You must try to keep work taken home relatively secure, to return all work related material upon the completion / termination of your contract; the company should be informed if information has got into wrong hands.
* Virus protection is up-dated daily when logging on; the system is backed up on a weekly basis and the CD taken off site.

This Policy is mandatory for all staff.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Signed | : |  |  | Date | : |  |
|  |  | Paul Fletcher  (*Managing Director*) |  |  |  |  |