

SecureCare

ELECTRONIC INFORMATION AND COMMUNICATIONS SYSTEMS POLICY

SecureCare (the “Company”) electronic communications systems and equipment are intended to promote effective communication and working practices within our organisation and are critical to the success of the Company.

This policy deals with the use (and misuse) of computer equipment, e-mail, the internet, telephones, i-pads, personal digital assistants (PDAs) and voicemail, but it applies equally to the use of fax machines, copiers, scanners, CCTV, and electronic key fobs and cards.

It outlines the standards we require users of these systems to observe, the circumstances in which we will monitor use of these systems and the action we will take in respect of breaches of these standards.

All staff are expected to protect the Company’s electronic communications systems and equipment from unauthorised access and harm at all times. Failure to do so may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

Equipment Security and Passwords

You are responsible for the security of the equipment allocated to, or used by, you, and must not allow it to be used by anyone other than as permitted by the Managing Directors.

If you have been issued with a laptop, PDA or i-pad, you must ensure that it is always kept secure, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

Systems and Data Security

You should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming the Company or exposing it to risk.

No device or equipment should be attached to the Company’s systems without the prior approval of Robert Stevenson. This includes any USB flash drive, MP3 or similar device, PDA or telephone. It also includes use of the USB port, infra-red connection port or any other port.

If you use laptops or wi-fi enabled equipment, you should be particularly vigilant about its use outside the office and take any precautions required by us from time to time against importing viruses or compromising the security of the system. The system contains information which is confidential to the Company and/or which is subject to data protection legislation. Such information must be treated with extreme care and in accordance with the Company’s Data Protection Policy.

E-mail Etiquette and Content

E-mail is a vital business tool, but an informal means of communication, and should be used with great care and discipline. You should always consider if e-mail is the appropriate means for a communication and correspondence sent by e-mail should be written as professionally as a letter or fax.

Messages should be concise and directed only to relevant individuals.

You should not send abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory e-mails. Anyone who feels that they have been harassed, bullied, or are offended by material received from a colleague via e-mail should inform Robert Stevenson.

You should take care with the content of e-mail messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. You should assume that e-mail messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

Should you receive a wrongly-delivered e-mail, you should return it to the sender. If the e-mail contains confidential information or inappropriate material it should not be disclosed or used in any way.

This Policy will be regularly reviewed and updated as necessary. The management team endorses these Policies and is fully committed to their implementation.

This Electronic Information and Communications Systems Policy has been approved & authorised by:

Signature:

Signed by: ROBERT STEVENSON
Position: DIRECTOR

Date:

Review date: