

# EMAIL AND INTERNET ACCEPTABLE USE POLICY

OF

## WINNS SECURITY SERVICES LIMITED

### 1 INTRODUCTION

WINNS SECURITY SERVICES LIMITED views the internet and the use of email as an increasingly important business tool. The purpose of this policy is to protect the quality and integrity of the company's electronic communications and to provide employees with standards of behaviour when using them. This document sets out guidelines for email and internet use by all employees to encourage the correct use of email and the internet in the business environment. Any breach of this policy or misuse of electronic communications may constitute a serious disciplinary matter and may lead to dismissal.

### 2 POLICY

It is the policy of the company to encourage the use of its email and internet services to share information, to improve communication and to prohibit unauthorised and improper use of these means of communication. Use of the internet and email facilities is permitted and encouraged where such use is suitable for business purposes only and supports the goals and objectives of the company and is to be used in a manner that is consistent with the company's standards of business conduct and as part of the normal execution of an employee's job responsibilities. Those who use the company's internet and email services are expected to do so responsibly and must comply with this policy. Personal use of company email accounts and the internet is expressly forbidden at all times.

### 3 GENERAL PRINCIPLES

The principles outlined in this policy apply to all electronic communications sent by employees and all use of the internet if using the company's access accounts or equipment.

### 4 ACCESS

4.1 The company reserves the right to designate those employees to whom it will provide access to the internet and email services and may revoke access at any time to persons who misuse the system. The company's computer equipment and systems must only be accessed and operated by those authorised to do so. Unauthorised use, intentional interference with the normal operation of the network or failure to comply with this policy will be regarded as gross misconduct and may lead to dismissal and possible criminal prosecution.

4.2 Internet access is controlled and the company reserves the right to prevent access to any sites it deems unacceptable. Any employee attempting to evade the controls instituted will be suitably disciplined and may be dismissed in appropriate circumstances.

## **5 VIRUSES**

All computers should use authorised and current anti-virus protection software. No unauthorised anti-virus software should be installed, transmitted or downloaded.

## **6 SECURITY**

6.1 All software downloaded to a company computer must be approved by a member of staff responsible for IT systems before installation to assure compatibility with software already installed on the computer. Problems may arise when unauthorised software is installed which is not compatible with the approved software. No disks may be brought in from an employee's home and used on the company's system at any time.

6.2 Subject to paragraph 6.1, employees must not download software or electronic files without implementing virus protection. All files attached to external email as well as files downloaded from the internet must be scanned. Users must report suspected incidents of software viruses or similar contaminants from email attachments and/or downloads from the internet immediately to a member of staff responsible for IT systems.

6.3 Passwords, encryption keys and other confidential information relating to the company's systems must not be transmitted over the internet or by email.

6.4 Employees must not change or use another person's files, output or user name for which they do not have express authorisation. Employees should use password protection or switch off their computer when away from it.

## **7 MONITORING**

By accessing the internet and email services through facilities provided by the company the user acknowledges that the company can monitor and examine all individual connections and communications. The company respects the privacy of internet and email users and will not monitor email or internet access activities without an employee's knowledge or without good cause. Any such monitoring will comply with the provisions of the Data Protection Act 1998.

## **8 PROHIBITED USE**

8.1 Employees must not view, store, transmit, upload, download or intentionally receive communications, web pages, files or documents that are or could be interpreted as intimidating, harassing or illegal or containing hostile, degrading, sexually explicit, pornographic, discriminatory or otherwise offensive material.

8.2 Employees must not send unsolicited emails, or email messages to multiple recipients nor use email for personal gain nor represent personal opinions as those of the company.

## **9 EMAIL USE**

As well as the many benefits of email, it is essential that all employees realise the following potential pitfalls:

9.1 it is not an informal communication tool, but has the same authority as any other communication to and from the company;

9.2 external emails should have disclaimers attached;

- 9.3 it should be regarded as published information;
- 9.4 emails are not confidential and can be read by anyone given sufficient levels of expertise;
- 9.5 binding contracts may be inadvertently created;
- 9.6 defamation of colleagues or other parties (deliberate or otherwise) may occur;
- 9.7 abrupt, inappropriate and unthinking use of language can lead to a bullying tone and possible offence to others, even harassment, for example, capitals are often interpreted as shouting;
- 9.8 consider whether a phone call may be a better way of discussing a complex or confidential matter.

## **10 BLOGGING, INSTANT MESSAGING AND USE OF SOCIAL NETWORKING SITES**

Keeping an online diary or weblog known as 'blogging', instant messaging and the use of social networking sites such as Facebook are viewed by the company as internet activities and are subject to the terms and conditions of this policy. Such activities must not be carried out during normal working hours and must not bring the company into disrepute. They must not directly refer to, nor indirectly insult or demean, the company or any employee, customer, client or director of the company and must not breach anti-harassment, defamation or discrimination legislation (age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage and civil partnership and pregnancy and maternity).

## **11 CONFIDENTIALITY**

- 11.1 Email can be inadvertently sent to the wrong address. It may also be read by someone other than the intended recipient. Caution must be exercised when communicating proprietary, confidentially sensitive information or information relating to the company when using email systems and users should ensure that such information is properly encrypted and that they have the authority to send it.
- 11.2 No client or customer related information should be sent over any public computer system without the prior written consent of the client or customer.

## **12 COPYRIGHT**

Employees must adhere to all intellectual property and copyright law. Employees must not upload, download or otherwise transmit any copyrighted materials belonging to parties outside the company without the copyright holder's written permission.

## **13 CONTRACTS**

Employees should be aware that contracts which bind the company can be created on the internet or by email. Employees must not enter into contracts or subscribe for, order, purchase, sell or advertise for sale any goods or services on the internet or by email, unless with the express authorisation of the company.



**14 DISCIPLINARY ACTION**

Any breach of this policy may be subject to disciplinary action, up to and including dismissal and may result in criminal prosecution.

**15 CONTACT PERSON**

Employees should contact JOHN DOWLER - GENERAL MANAGER, if they have any queries about any aspect of the policy.