**Acceptable Use Policy**

**Doc A8.1**

**Version: 1.0**

Publication Date: January 01, 2019

Current Status: Published

Author(s): Michael Woolard

Last Reviewed: Michael Woolard

**Table of Contents**

1 Acceptable Use Policy 3

1.1 Overview 3

1.2 Internet Acceptable Use Policy 3

1.3 Usage of EMAIL and Communication Activities 5

1.4 Compliance 6

2 Document Control and Approval 7

2.1 Distribution 7

2.2 Version Information 7

# Acceptable Use Policy

## Overview

The Company provides access to the vast information resources of the Internet to help you do your job faster and smarter, and be a well-informed business citizen. The facilities to provide that access represent a considerable commitment of company resources for telecommunications, networking, software and storage. This acceptable use policy is designed to help you understand the Company’s expectations for the use of those resources in the particular conditions of the Internet, and to help you use those resources wisely.

While we’ve set forth explicit requirements for Internet usage below, we’d like to start by describing our Internet usage philosophy. First and foremost, the Internet is a business tool for the Company provided to you at significant cost. That means we expect you to use your Internet access *primarily* for business-related purposes, i.e., to communicate with customers and suppliers, to research relevant topics and obtain useful business information. We insist that you conduct yourself honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as you would in any other business dealings. To be absolutely clear on this point, all other Company policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of company resources, sexual harassment, information and data security, and confidentiality.

This policy applies to every individual who uses Company information assets and it sets out what the Company considers to be the acceptable use of those assets.

## Internet Acceptable Use Policy

Company User IDs, websites and e-mail accounts may only be used for Company-sanctioned communications.

The use of Company computer resources is subject to local jurisdictional law and any abuse will be dealt with appropriately.

Users may not visit Internet sites that contain obscene, hateful or other objectionable material, shall not attempt to bypass Company content control technology where it is installed and shall not make or post indecent remarks, proposals or materials on the Internet.

The display of any kind of sexually explicit image or document on any company system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.

Users shall not solicit e-mails that are unrelated to business activity or which are for personal gain, shall not send or receive any material which is obscene or defamatory or which is intended to annoy, harass, or intimidate another person, and shall not present personal opinions as those of the company.

Users may not upload, download, or otherwise transmit commercial software or (other than in the ordinary course of business) any copyrighted materials belonging to the company or any third parties, and may not reveal or publicize confidential information.

Users may not download software from the Internet or execute or accept any software programs or other code on the Internet unless it has first been authorized by Technical Services in accordance with the Company policies and procedures.

Any software or files downloaded via the Internet into the Company network become the property of the Company. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

No user may use the Company’s Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

Each member of Staff using the Internet facilities of the Company shall identify himself or herself honestly, accurately and completely (including one’s Company affiliation and function where requested) when participating in any internet related activity, or when setting up accounts on outside computer systems.

Only those Staff or officials who are duly authorized to speak to the media, to analysts or in public gatherings on behalf of the Company may speak or write in the name of the Company to any social media, newsgroup or chat room. Other Staff may participate in social media, newsgroups or chats in the course of business *when relevant to their duties*, but they do so as individuals speaking only for themselves. Where an individual participant is identified as a member of Staff or agent of the Company, the Staff member must refrain from any unauthorized political advocacy and must refrain from the unauthorized endorsement or appearance of endorsement by the Company of any commercial product or service not sold or serviced by the Company, its subsidiaries or its affiliates. Only those managers and company officials who are authorized to speak to the media, to analysts or in public gatherings on behalf of the Company may grant such authority to newsgroup or chat room participants.

The Company retains the copyright to any material posted to any social media, forum, newsgroup, chat or web page by any Staff in the course of his or her duties.

Staff are reminded that where access is granted, social media, chats and newsgroups are public forums where it is inappropriate to reveal confidential Company information, customer data, trade secrets, and any other material covered by existing Company secrecy policies and procedures. Staff releasing protected information via a newsgroup or chat – whether or not the release is inadvertent – will be subject to all penalties under existing data security policies and procedures.

Users will not carry out any other inappropriate activity as identified from time to time either in writing or verbally by the Company and, although limited use of Company facilities for minor personal administrative tasks such as (for example) banking is permitted, will not waste time or resources on non-Company business.

It remains the responsibility of Staff with Internet access to take particular care to understand the copyright, trademark, libel, slander and public speech control laws of all countries in which the Company maintains a business presence, so that our use of the Internet does not inadvertently violate any laws which might be enforceable against us.

Staff may use their Internet facilities for non-business research or browsing during their designated lunch time or other breaks, or outside of work hours, provided that all other usage policies are adhered to. However, caveats do apply:

* Since a wide variety of materials may be deemed offensive by colleagues, customers or suppliers, it is a violation of Company policy to store, view, print or redistribute any document or graphic file that is not directly related to the user’s job or the Company’s business activities. In conjunction with this, Staff with Internet access may download only software with direct business use, and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license. All software must be approved by Technical Services prior to installation.
* Staff with Internet access may not use Company Internet facilities to download entertainment software or games, or to play games against opponents over the Internet.
* Staff with Internet access may not upload any software licensed to the Company or data owned or licensed by the Company without explicit authorization from the manager responsible for the software or data.
* Video and audio streaming and downloading technologies represent significant data traffic which can cause network congestion. Video and audio downloading is permitted, however this should be used sparingly. In some cases additional restrictions may be put in place to ensure essential business traffic is not disrupted by data streaming.

## Usage of EMAIL and Communication Activities

Company e-mail facilities may not be used for sending defamatory e-mails, or using e-mail for harassment, unauthorized corporate purchases, or for publishing views and opinions (defamatory or otherwise) about employees, workers, suppliers, partners or customers of the Company.

Company e-mail may only be used for the communication of official business information or appropriate personal information. Employees will have no privacy rights over e-mails sent using Company e-mail.

Outgoing e-mail attachments must be protected in line with their classification, using cryptographic controls

Users must not open incoming e-mail attachments that originate with unknown third parties or that, even if they appear to have been sent by a known party (however important that party my appear), were not expected. These attachments may contain viruses, worms or Trojans and any such e-mails must be deleted immediately, and on no account should they be forwarded, or copied on, to anyone, whether inside or outside the network. Where more than three such emails are received within a 24-hour period, the instance must be reported to the Technical Services Support team for further investigation.

Viruses and hoax virus messages: users are required to report any third party e-mail messages they receive about viruses to Technical Services Support team, by telephone or in person, and on no account should it be forwarded, or copied on, to anyone, whether inside or outside the network.

Internal group email addresses may not be given to third parties, unless those third parties have entered into an appropriate confidentiality agreement.

Users are required to use their discretion to limit as far as practically possible the use of group e-mail addresses, to limit copying to unnecessary recipients, to restrict use of the “reply to all” function, and restrict the use of the blind copying feature.

Users are required to comply with the Incident Reporting Procedure. Employees are required to delete non-essential e-mail messages as soon as possible and, on a regular basis, to clear e-mail boxes of correspondence that is no longer required.

Use of Passwords must be in accordance with Access control policy.

E-mail is a powerful tool for communication, but when overused or used inappropriately can become ineffective and a drain on the time of those receiving the e-mails. Judgement should be used to ensure other forms of communication are used where e-mail may not be the best method.

## Compliance

Use of Internet / intranet / e-mail / instant messaging may be subject to monitoring for reasons of security and / or network management and users may have their usage of these resources subjected to limitations by the Company.

The distribution of any information through the Internet (including by e-mail, instant messaging systems and any other computer-based systems) may be scrutinized by the Company and the Company reserves the right to determine the suitability of the information.

We reserve the right for authorized users to inspect any and all files stored in private areas of our network in order to assure compliance with policy.

The Company may use independently-supplied software and data to identify inappropriate or sexually-explicit Internet sites. We may block access from within our networks to any sites that we deem unacceptable. If you find yourself connected accidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.

No member of Staff may use the Company’s Internet facilities knowingly to disable or overload any computer system or network.

It is prohibited to circumvent any system intended to protect the privacy or security of the system, another user, or Company information.

The Company reserves the right under this policy to limit Internet access to those Staff who demonstrate a legitimate business need.

Only those Internet services and functions with documented business purposes for this Company will be enabled at the Internet firewall.

Breaches of the requirements in this policy may be dealt with under the Company disciplinary procedure.

# Document Control and Approval

The Chief Information Security Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff and is the published version.

Signature: Executive Manager Signature Date: 01.01.2019

## Distribution

|  |  |
| --- | --- |
| **Name** | **Role** |
| *Intranet* | *Distribution to all staff* |

## Version Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Details** |
| 0.1 | 11/28/18 | M.Woolard | First draft |
| 0.2 | 12/07/18 | M.Woolard | Second draft |
| 1.0 | 01/01/19 | M.Woolard | First published |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 