<< Organisation Logo>>

<< Internet Usage Policy >>

Version: 1.0
Date

Version: xx　　　　　　　　**Date: xx**　　　　　**[Organisation] Name: xx**

Security Level: Internal　　　　　**Page 1 of 5**
NetHost Legislation- Cyber Essentials and ISO Standard Management System Certification Company, Scotland/England

info@nethostlegislation.co.uk,　　　　　　　　　　　**www.nethostlegislation.co.uk**

Revision History

Date	Version	Author	Summary of Changes

Approvals

Name	Signature	Title	Issue Date	Version

Version: xx   **Date: xx**   **[Organisation] Name: xx**

Security Level: Internal   **Page 2 of 5**
NetHost Legislation- Cyber Essentials and ISO Standard Management System Certification Company, Scotland/England

info@nethostlegislation.co.uk,   **www.nethostlegislation.co.uk**

Contents

Contents

INTRODUCTION

DOCUMENT PURPOSE

Access to the Internet is provided to all staff for work purposes only and is an essential requirement for the daily operations of the business, however staff must be aware that there are also certain inherent risks associated with using the Internet.

There has various systems in place to reduce the number of threats such as spyware, malware, trojans, pop-ups, viruses, worms and other malicious software that can inadvertently be downloaded by staff.

This purpose of this policy is to help staff navigate through the Internet as safely as possible and to minimise the risk of compromise posed by these threats.

SCOPE

This polciy only pertains to the corporate Internet gateway. It does not cover Internet gateways provided by other external 3rd parties.

POLICY

Below are statements that should be followed by all staff.

Policy Statements

No:	Statements
	Do not download or open attachments unless absolutely necessary. Ensure wherever possible that the site you are downloading from is reputable.
	Do not open EXE, BAT, VBS, and SCR type attachments without performing an anti-malware scan, since they are common vectors for virus/malware infections.
	Do not use Web-based e-mail systems (e.g. Google Mail, Yahoo, etc) for the communication of any sensitive or business information.
	Access to and downloading of content from sites which are deemed as offensive.
	Producing or downloading information which is considered to be of a threatening or violent nature.
	Access to and downloading of content from sites which are considered to be illegal.
	Confidential information should not be sent over the Internet without using PGP-enabled

	email or use other secure methods of encryption communication like VPNs
	Any information that [organisation] do not want to be public knowledge should not be sent to any websites unless absolutely necessary