INFORMATION SECURITY POLICY

INTERNET ACCEPTABLE USE

ISO 27002	7.1.3
Author:	Chris Stone
Owner:	Ruskwig
Organisation:	TruePersona Ltd
Document No:	SP-7.1.3
Version No:	1.0
Date:	10th January 2010

Document Control

Document Storage

Document Title Internet Acceptable Use
Document Location C:\www\Ruskwig\docs\iso-27002\Internet AUP - RW.doc

Version History

Version No	Version Date	Author	Summary of Changes
1.0	10/01/2010	Chris Stone	First Issue

Approvals

Name	Title	Date of Approval	Version No
Chris Stone	Director	10/01/2010	1.0

Distribution

Name	Title	Date of Issue	Version No
Everyone	Internet	16/01/2010	1.0

Contents

DOCUMENT CONTROL 2

Document Storage 2

Version History 2

Approvals 2

Distribution 2

CONTENTS 3

1. PURPOSE 4

2. SCOPE 4

3. RISKS 4

4. POLICY 4

4.1 Corporate policy on use of the Internet 4
4.2 Monitoring of Internet use 5
4.3 Personal use of the Internet 6
4.4 Software downloads and uploads 6
4.5 Purchasing of goods or services 7
4.6 Instant Messaging 7
4.7 Participation in public Internet forums 7
4.8 Computer viruses and malicious programs 7
4.9 Masquerading 7
4.10 Legal Compliance 7

5. ENFORCEMENT 8

1. Purpose

1.1 Internet access is provided to staff to assist them in carrying out their duties efficiently and effectively. This facilitates access to a vast range of information available on the world-wide web and the communication with people outside of the organisation.

1.2 This policy is in place to ensure effective use of time, to prevent illegal and inappropriate use of the Internet.

2. Scope

2.1 This policy applies to all staff and employees of the organisation.

2.2 All users of the organisation's IT facilities must understand and use this policy. Users are responsible for ensuring the safety and security of the organisation's systems and the information that they use or manipulate.

2.3 All users have a role to play and a contribution to make to the safe and secure use of the Internet.

3. Risks

3.1 A large number sites exist on the Internet that contain inappropriate content and it is important that this content is not downloaded to the organisation's computer systems. Many other sites contain malicious software which could harm the organisations computer systems if deliberately or inadvertently downloaded.

3.2 There is also a potential for the loss of productivity if staff spend unacceptably large amounts of time surfing the Internet.

4. Policy

4.1 Corporate policy on use of the Internet

4.1.1 The organisation's Internet access is primarily for business use.

4.1.2 Occasional and reasonable personal use of the Internet is permitted in your own time subject to the conditions set out in the organisation's security policies.

4.1.3 When using the organisation's Internet access facilities you should comply with the following guidelines

DO

- Do keep your use of the Internet to a minimum
- Do check that any information you access on the Internet is accurate, complete and current.
- Do check the validity of the information found.
- Do respect the legal protections to data and software provided by copyright and licenses.
- Do inform ICT Services immediately of any unusual occurrence.

DO NOT

- Do not visit any website that is perceived to be potentially offensive, this will include websites with pornographic, racist, sexist, ageist, homophobic, content or websites that promote religious hatred.
- Do not download text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity.
- Do not download software from the Internet and install it upon the Organisation's computer equipment.
- Do not use the Organisation's computers to make unauthorised entry into any other computer or network.
- Do not disrupt or interfere with other computers or network users, services, or equipment. Intentional disruption of the operation of computer systems and networks is a crime.
- Do not represent yourself as another person.
- Do not use Internet access to transmit confidential, political, obscene, threatening, or harassing materials.
- Do not publish or post defamatory or libellous material.

4.1.4 A corporate Internet filter is utilised to prevent specific types of websites being accessed.

4.1.5 Websites which need to be accessed to conduct the organisation's business but are blocked can be made available by contacting the IT Service Desk. Authorisation will be required before access is granted.

4.1.6 Accidental viewing of materials which infringes this policy should be reported according to the Information security incident reporting procedure.

4.2 Monitoring of Internet use

4.2.1 All content viewed is scanned for viruses and offensive material.

4.2.2 Use of the Internet is recorded and may be monitored. It is possible to identify Internet sites visited by individual users.

4.2.3 The organisation reserves the right to inspect any files at any time during investigations where there is suspected misuse and to withdraw access to the Internet.

4.3 Personal use of the Internet

4.3.1 Personal use is defined as any activity that is not work-related or necessary in the performance of duties connected to your employment.

4.3.2 Staff may use on an occasional basis the organisation's computers for personal use to access the Internet.

4.3.3 Staff who use the organisation's computers for personal use to access the Internet must accept, as a condition of doing so, that their activity may be monitored.

4.3.4 Staff using the organisation's computers waive any rights to privacy regarding personal information on the organisation's computers.

4.3.5 The personal use of the Internet for any purpose must be in the employee's own time and must not interfere with employee productivity.

4.3.6 Users should seek to keep any costs incurred as a result of personal use of the Internet to a minimum.

4.3.7 No liability can be accepted by the organisation for any loss that an individual may suffer as a result of personal use of the organisation's computers.

4.3.8 Support must not be requested from other employees for personal use of the Internet.

4.3.9 Subscription to e-mail mailing lists or list servers for personal purposes is not allowed.

4.3.7 The playing of Internet computer games is not allowed.

4.3.9 Using the Internet for personal purposes must comply with the principles set out in this security policy. Failure to comply with the policy may lead to disciplinary action.

4.4 Software downloads and uploads

4.4.1 The organisation has adopted a corporate standard desktop system. You are not allowed to download programs or software (including screen savers and wallpaper) from the Internet including programs or software available for trial purposes.

4.4.2 If programs or software available on the Internet are required for a genuine business need you must produce a business case and contact the IT Department

who will make the necessary arrangement to acquire and arrange for the installation of the programs or software.

4.5 Purchasing of goods or services

4.5.1 The purchasing of goods or services via the Internet is subject to the organisation's Financial procedures. These must be consulted to determine which goods and services it is permissible to purchase.

4.6 Instant Messaging

4.6.1 The use of Internet Instant Messaging tools is forbidden from the organsiations PCs and Networks. The lack of formal controls concerning data transfer and logging of messages prohibit their use.

4.7 Participation in public Internet forums

4.7.1 An Internet forum is a web application for holding discussions and posting user generated content. Internet forums are also commonly referred to as Web forums, message boards, discussion boards, discussion forums, bulletin boards, or simply forums.

4.7.2 The use of work related Internet forums for professional or technical purposes is permitted.

4.7.3 You must make every attempt to avoid bringing the organisation's name into disrepute or to adversely affect its reputation, customer relations or public image.

4.7.4 Personal use of public Internet forums should not be conducted using the organisation's IT equipment.

4.8 Computer viruses and malicious programs

4.8.1 Computers can be infected by viruses and malicious programs by just visiting a webpage.

4.8.2 If you think you have a computer virus report it to the IT Service Desk immediately.

4.9 Masquerading

4.9.1 It is an offence to masquerade as another person on the internet and post articles in another person's name.

4.10 Legal Compliance

4.10.1 The Internet must be used for lawful purposes only, and must comply with relevant legislation.

4.10.2 You be placing yourself at risk of prosecution if unlawful action is involved.

4.10.3 Electronic communications and files are admissible in court as evidence. Do not write anything about anybody that you cannot prove and evidence.

5. Enforcement

5.1 If any member of IT staff is found to have breached this policy, they may be subject to disciplinary action.

5.2 If any user is found to have breached this security policy, they may be subject to disciplinary action.

5.3 Any violation of the policy by a temporary worker, contractor or supplier may result in the termination of their contract or assignment.