INFORMATION SECURITY POLICY

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

Version History

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

Approvals

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

Distribution

Name	Title	Date of Issue	Version No
Everyone	Internet	10/01/2010	1.0

Contents

1. Purpose

1.1 Email is provided to staff to assist them in carrying out their duties efficiently and effectively. Email enables effective and efficient communication with other members of staff, other companies and partner organisations

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

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 email.

3. Risks

3.1 Emails may contain inappropriate content that should not be viewed by users.

3.2 Emails may contain malicious code which has the potential to access or damage data or forward data to a third party

3.3 There is also a potential for the loss of productivity if staff spend unacceptably large amounts of time sending emails.

4. Policy

4.1 Corporate policy on use of email

4.1.1 The organisation's email facilities are primarily for business use.

4.1.2 Occasional and reasonable personal use of email 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 electronic mail facilities you should comply with the following guidelines

DO

- Do check your electronic mail daily to see if you have any messages.
- Do include a meaningful subject line in your message.
- Do check the address line before sending a message and check you are sending it to the right person.
- Do delete electronic mail messages when they are no longer required.
- Do respect the legal protections to data and software provided by copyright and licenses.
- Do take care not to express views, which could be regarded as defamatory or libellous.

DO NOT

- Do not print electronic mail messages unless absolutely necessary.
- Do not expect an immediate reply, the recipient might not be at their computer or could be too busy to reply straight away.
- Do not forward electronic mail messages sent to you personally to others, particularly newsgroups or mailing lists, without the permission of the originator.
- Do not send excessively large electronic mail messages or attachments.
- Do not send unnecessary messages such as festive greetings or other non-work items by electronic mail, particularly to several people.
- Do not participate in chain or pyramid messages or similar schemes.
- Do not represent yourself as another person.
- Do not use electronic mail to send or forward material that could be construed as confidential, political, obscene, threatening, offensive or libellous.

4.1.4 A corporate email filter is utilised to prevent emails being delivered which may contain inappropriate or malicious content.

4.1.5 Emails 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 Email use

4.2.1 All electronic mail coming into or leaving the organisation is scanned for viruses and offensive material.

4.2.2 The use of email is recorded and may be monitored. It is possible to identify the senders, recipients and content of email.

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 email.

4.3 Personal use of email

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 send and receive email.

4.3.3 Staff who utilise one of the organisation's computers for personal use to send and receive email access 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 email any purpose must not be excessive. It should not count as working time and must not interfere or detract from the organisation's business or work. It should not distract any other individual from their work.

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

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

4.3.9 Using email 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 Phishing

4.4.1 Take care when viewing emails not to be deceived by phishing. Reputable organisations will not ask you to run software or click on a link to verify your password.

4.5 Purchasing of goods or services

4.5.1 The purchasing of goods or services via email is subject to the organisation's financial regulations. 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 organisation's PCs and Networks. The lack of formal controls concerning data transfer and logging of messages prohibit their use.

4.7 Computer viruses and malicious programs

4.7.1 Computers can be infected by viruses and malicious programs by opening an attachment to an email or just visiting a link to a webpage contained within the email.

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

4.8 Masquerading

4.8.1 It is an offence to masquerade as another person via email and to send emails in another person's name.

4.9 Legal Compliance

4.9.1 The use of email must for lawful purposes only, and must comply with relevant legislation.

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

4.9.3 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.