joining up journeys SPT

Strathclyde Partnership for Transport

Internet and Email policy

Policy

1. Statement of Policy

INTRODUCTION

The Business Need for Internet Access

1.1 This policy has been developed to ensure that everyone using SPT computer facilities (including PC's, laptops, PDA's etc.) is aware of the rules that must be followed.

1.2 SPT recognises that access to both e-mail and the Internet is critical to the work carried out by Staff and the Partnership.

1.3 Many of our customers, partners and suppliers have an expectation that they can deal with us through these mediums.

1.4 E-mail and the Internet are key components in central government targets for the delivery of Electronic Government.

Why a Policy?

1.5 Because of the open nature and ready availability of e-mail and Internet services, there are potential dangers to SPT. These could arise from malicious intent, carelessness, complacency or misuse. Preventing these risks occurring is of paramount importance and requires SPT to adopt a policy on the use of these facilities.

1.6 This document is intended to clearly define the conditions of use of the Internet and e-mail for Staff. The policy should be read in conjunction with SPT's 'IT & Information Security Policy' which defines the responsibilities of all users of ICT Services for computer security. A copy of the policy is available via the SPT Intranet site or on request from the Service Desk.

1.7 A separate 'SPT ICT Users Guide' is available to all Staff. The document provides advice on best practice whilst using SPT's computer facilities. Copies of the guide are available via the Intranet site or can be obtained from the Service Desk on request.

1.8 It should be noted that references to 'e-mail' within this document apply to both internal and external use of the medium. Unless specifically excluded, references to the Internet should also be taken to include the Intranet, Electronic Bulletin Boards, online discussion forums and similar electronic information exchanges.

1.9 In the event of actual or suspected misuse of e-mail or the Internet, authorisation may be withdrawn from an individual. In addition action may be taken against the member of Staff through the disciplinary process.

1.10 This policy will be subject to amendment in response to changing circumstances. Should this occur, you will be advised accordingly. If you have any queries regarding access to the Internet or e-mail please contact the Service Desk on ext 3731 or servicedesk@spt.co.uk .

2. Scope of Policy

All Employees, Contractors and Agency staff authorised for Internet access and e-mail must comply with this policy. It is essential that standards relating to accessing appropriate content and maintaining the good reputation of SPT are observed.

3. Legislation

None.

Procedures

4. Rules

Security Principles

4.1 It is essential that this document is used in conjunction with SPT's IT & Information Security Policy, which defines rules for the protection of information and the technology used to store and retrieve it. It also defines the relevant legislation.

4.2 Key principles of the Security Policy which are relevant to e-mail and Internet usage include:-

- Any violation of rules and procedures should be reported to the Senior Technology Solutions Advisor or your Line Manager.
- Deliberate violation of the rules and procedures in the policy **will result in disciplinary action**.
- It is your duty to be aware of your legal responsibilities and to comply with the legislation. If you are unsure, ask.
- Access to computer systems is controlled by appropriate levels of security and authorisation. Do not disclose your password or security details.
- Do not leave your computer unattended while logged in.

5. Responsibilities

All Employees, Contractors and Agency staff authorised for Internet access and/or e-mail must comply with this policy.

6. Definitions

None.

7. Arrangements

7.1 CONDITIONS OF USE

Access to Services

7.1.2 Internet and E-mail facilities will only be provided to authorised staff and Partnership Members. Requests for access to these services must be formally requested through the Service Desk.

7.1.3 SPT connects to its Internet Service Provider (ISP) through a Firewall configuration.

7.1.4 Modem connections from networked workstations are specifically prohibited unless agreed with the Senior Technology Solutions Advisor.

7.1.5 Connections to the Internet using SPT owned laptops must be configured by Technology Solutions personnel. Staff should not change these settings.

7.1.6 Prior to an Internet access account being set up, formal authorisation from the User's Supervisor/Manager is required. Forms to request access are available from the Intranet. A minimum notice period of 3 days is required for a request to be processed.

Purpose and Use

7.1.7 The e-mail and Internet service is installed expressly for the purpose of supporting SPT's business activities. Access for personal use within core hours or whilst clocked in the flexi-system (except during the official tea-break) is not permitted, nor is the personal use of the Internet which could contravene this policy in any way.

7.1.8 SPT is prepared to allow limited personal use of the services to employees and Partnership Members subject to the following conditions:-

- Access can be monitored to measure adequacy of service and inappropriate use as defined by this policy.
- All guidelines (as outlined below) apply to any use of e-mail or Internet access for personal use.
- Access should only be undertaken in the employee's own time, not when they should be doing their normal work.
- Under no circumstances should the service be used to operate or support a business or private venture.
- Under no circumstances should the service be used for any purpose that may be considered illegal or mischievous.
- Use of the service in such a way as to threaten the normal operation of SPT's business, or to damage the reputation of SPT, will result in action, which may range from temporary or permanent withdrawal of access, to disciplinary action under SPT's disciplinary procedure.

7.1.9 SPT's Internet service and e-mail may not be used for transmitting, retrieving or storing any communication of a discriminatory or harassing nature or materials that are offensive, obscene, pornographic or sexually explicit. Should there be evidence of any abuse of this nature disciplinary action will be taken.

7.1.10 Users must not use or transmit abusive, profane or offensive language on or through SPT's intranet, Internet or e-mail systems. Failure to comply may result in disciplinary action being taken.

7.1.11 SPT makes use of specialised software to monitor and control access to undesirable content. Technology Solutions monitor and log access to Internet sites. Details of web sites visited, pages accessed (or attempted), and files downloaded are recorded.

7.1.12 No User may use SPT's Internet or e-mail facility to deliberately propagate any virus, worm, Trojan horse, trap-door program or other malicious code.

7.1.13 No User may knowingly use SPT's Internet or e-mail facilities to disable or overload any computer system or network, or to attempt to disable, defeat or circumvent any system intended to protect the privacy or security of another user.

7.1.14 No User may install additional Internet or e-mail related software, or change the configuration of existing software without the authorisation of their Director and the Senior Technology Solutions Advisor.

7.1.15 Where additional authentication and password controls are installed for Internet and E-mail access, Users must ensure that these remain confidential and are not disclosed to others.

7.1.16 To help prevent unauthorised users gaining access to the Internet, computers should not be left logged into the network or modem and unattended for any length of time.

7.1.17 Accounts will be disabled for any staff leaving employment with SPT. Managers must inform HR of any staff movements. HR are responsible for passing this information onto Technology Solutions for amendment.

7.2 DOWNLOADING AND UPLOADING FILES AND DATA

7.2.1 No User should download any software from the Internet without first seeking approval from Technology Solutions. This excludes static data or bulletin information.

7.2.2 Any data or software must only be for direct business use. The User is responsible for ensuring registration of any necessary licence and informing the Senior Technology Solutions Advisor of licence compliance. Users should be aware of the law relating to the Copyright, Design and Patents Act 1988 and the Copyright and Related Rights Regulations 2003.

7.2.3 No user may use SPT's Internet facility to access, download or distribute pirated software or data.

7.2.4 Internet facilities will not be used to download or play entertainment software or games. No video or picture images are to be downloaded unless there is an explicit business-related use for the material and no copyright infringed. Users should check with the Service Desk.

7.2.5 No user may upload software licensed to SPT or data owned or licensed by SPT to either the Internet or any recordable media.

7.2.6 No User may download, copy or transmit to third parties the works of others without their permission as this may infringe copyright.

7.2.7 It is strictly forbidden to download from the Internet, or upload from a memory device, screensavers, applications, videos, music, pictures and wallpapers onto SPT Computers.

7.3 VIRUS PROTECTION

7.3.1 SPT uses Virus protection software on all networked and laptop computers. The software is configured to intercept any viruses in e-mail attachments and files downloaded from the Internet. The Software is updated daily to ensure that the most recent detection profiles are available.

7.3.2 Although the software provides assurances it must not be a substitute for extra vigilance when using the Internet and E-mail systems.

7.3.2 Technology Solutions reserve the right to delete suspect e-mail. E-mails containing inappropriate material or references, or containing attachments, which are inappropriate, or contain viruses, may be blocked at the Firewall. The Senior Technology Solutions Advisor may investigate these contraventions of policy and will refer these to the Chief Internal Auditor for investigation.

7.3.3 The 'SPT ICT User Guide' provides additional and effective rules to observe to minimise the risk of introducing viruses. Users should make themselves aware of these guidelines.

7.4 THE USE OF E-MAIL

7.4.1 Do not assume privacy for any Internet communications of any kind. E-mails and/or files can be posted or forwarded to other Internet users around the world without the user's knowledge or permission.

7.4.2 Technology Solutions may monitor the use of e-mail and content (see paragraph 6). Abuse or misuse of the service may lead to disciplinary action. Defamatory, libelous, abusive, sexist or racist comments in e-mail may render the sender personally liable to civil or criminal action.

7.4.3 Any messages or information sent by an Employee or Member are statements that reflect on SPT. All Users should be aware that their views will be construed as representing SPT. All e-mails include a disclaimer. It should be noted that a disclaimer does not legally divorce the legal connection between the sender and SPT. Messages may result in the constitution of a contract between SPT and a third party.

7.4.4. The 'Out of Office' facility is to be used in a professional and Customer Focused capacity. It is there to notify colleagues and customers of your availability and should detail a return date and alternative contacts. The auto-delete option is not to be used.

7.4.5 Abuse or misuse of the e-mail system may result in the appropriate disciplinary proceedings being instigated.

7.4.6 Staff are reminded that mailboxes can be shared for colleagues who are on long term leave.

7.5 MONITORING OF USE

7.5.1 The E-mail and Internet services are installed expressly for the purpose of supporting SPT's business. To maintain security and integrity, Technology Solutions staff may investigate monitoring logs for the purpose of:-

- Detecting viruses.
- Prevention of unauthorised access to SPT systems.
- Inappropriate use of the Internet or E-mail as defined by this policy.
- Detecting unusual trends in use of Internet or E-mail services.

7.5.2 All information held on SPT systems is considered the property of SPT and may be subject to monitoring.

8. Training

8.1 Each new employee is made aware of his or her obligations to ensure proper use of Internet and E-mail facilities during SPT's induction-training program. This includes Staff being told of the existence of the Security Policy, the Email and Internet Policy and the 'Good Practice Guide for Computer Users'. Training on the proper use of ICT is available from TS on request.

8.2 Training requirements are reviewed on a regular basis to take account of the needs of the individual, and to ensure that staff are adequately trained in the use of technology.

8.3 Corporate IT training is the responsibility of the Human Resources & Organisational Development Directorate. Where training is required for a specific application this may be carried out in consultation with the Users Manager.

9. Review

The Senior Technology Solutions Advisor is responsible for reviewing this policy. This policy is to be reviewed under the following circumstances;

- Annually
- In the event of a major change that may affect the security of the IT infrastructure.

10. Approval (signature and date)

Sign;

Print;

Dean Drew

Date; **12/04/10**

Designation; **Senior Technology Solutions Advisor**