APPENDIX 4

Strathclyde Partnership for Transport

Digital Assets

Acceptable Use Procedures

Contents

Change Log

Page	Version	Date	Brief summary of changes	Initials
All	1.0	Jan-19	Evolution of Internet and Email Policy	CT

1. Introduction

This document establishes the mandatory guidance within SPT covering the appropriate use of Digital technology assets (such as PC's, Laptops, Tablets, Mobile Phones etc).

2. Scope

These procedures apply to all SPT employees and members, including temporary staff, suppliers and contractors, with access to Digital assets, SPT e-mail, intranet and internet resources. Access to all systems and resources are tightly controlled by technology asset owners or the Digital Department.

3. Acceptable Use of Digital Assets

Expectation of Privacy

SPT may monitor e-mail, digital technology and internet resources; including the creation, entry, receipt, storage, accessing, viewing or transmission of data. As with all other SPT property, SPT reserves the right to monitor, investigate and/or search for any and all information contained in SPT computer systems (databases, data file systems, data archives, SPT issued personal computers, Web/Internet/Intranet sites, etc.) without the consent of the employee at the direction of the SPT Strategy Group. Any information retained on SPT resources and/or facilities may be disclosed to outside parties or to law enforcement authorities.

Representing SPT

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.

4. Email and Internet

Usage

SPT provides employees with access to business e-mail, digital technology and internet resources as tools to assist in accomplishing business objectives. Users of e-mail, computer and internet resources are required to use these tools appropriately in conducting SPT business, regardless of whether or not it is during business hours, and whether or not from SPT premises.

Personal Use

Other than occasional personal use, SPT e-mail, software, computers, internet tools and all SPT provided technology resources may be used only for legitimate organisation-related activities. Occasional personal use means, during authorised breaks only, infrequent, incidental use that is professional and does not interfere with SPT business, the performance of the User's duties, or the availability of technology resources. All use of SPT-provided e-mail, computers, software and internet resources – including all personal use – is subject to this guidance.

SPT provides access to a 'Guest' Wi-Fi for staff and visitors. Whilst this can be used for access to non-business internet sites, it should not breach any other part of these procedures or other SPT policies.

Personal email is not to be accessed from within the SPT network or using any SPT device.

SPT Information

SPT information must not to be forwarded to personal email accounts unless approved in advance by SPT's Data Processing Officer or Information Governance Officer.

Harassment-Free Usage

Users are absolutely forbidden from using SPT e-mail, computer and internet resources in any way that may be construed to violate SPT's bullying and harassment policy. This prohibition includes but is not limited to transmitting, receiving, printing and/or displaying sexually explicit or offensive images, messages, cartoons, jokes, ethnic or religious slurs, racial epithets, or any other statement or image that might be construed as harassment or disparagement on the basis of age, disability, gender reassignment, marriage or civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation, or any other status protected by law. Users are required to take all reasonable steps to avoid transmission and eliminate receipt from known sources of all potentially offensive material.

Unlawful Activities

SPT e-mail, computer and internet resources may not be used to violate any local, national, or foreign civil or criminal laws, including, without limitation, the copyright, patent and regulations of any country. Unlawful activity includes the participating or facilitating in the distribution of unlawful materials. Users likewise may not upload, post, e-mail, copy or otherwise transmit any data that is threatening, malicious, tortuous, defamatory, libellous, obscene, or invasive of another's privacy. Users also may not upload, download, post, e-mail, copy or otherwise transmit any material that contains software viruses or any other computer code, files, or programs designed to interrupt, destroy, or limit the functionality of any computer software, hardware, or telecommunications equipment.

5. Computing

Usage

Other than occasional personal use, e-mail, software, computers, internet tools and all SPT provided technology resources may be used only for legitimate business-related activities. Occasional personal use means, during authorised breaks only, infrequent, incidental use that is professional and does not interfere with SPT business, the performance of the User's duties, or the availability of technology resources. All use of SPT-provided e-mail, computers, software and internet resources – including all personal use – is subject to this document. All computers and mobile devices should be locked when left unattended.

SPT Information

In order to prevent against loss, SPT information should not be stored on local drives. All information should be saved to a network file server as soon as is practical. Sensitive SPT information must not to be stored on personal devices.
SPT information is not to be stored on any cloud service e.g. Google docs, Dropbox, unless approved in advance by SPT's Data Processing Officer or Information Governance Officer.

Security Software

Employees are not permitted to disable, remove or interfere with any security tool installed on SPT computers (e.g. anti-malware, firewalls). Employees must not install their own security software on computers unless approved in advance by SPT's Digital department management.

Infringement of Proprietary Rights

SPT e-mail, computer and internet resources may not be used to violate proprietary rights, including copyright, trademark, trade secret, patent, rights of publicity, or any other intellectual property rights. For example, users may not post, upload, download, transmit, distribute, copy, or engage in any "file-sharing" of any data or files (including software, music, audio-visual clips, movies, etc.) unless such activity is consistent with all applicable licenses and approved in advance by the SPT Strategy Group. Likewise, users may not install software from the internet or other sources onto SPT-provided computers unless approved in advance

by SPT's Digital department management; and provided that such use of the software is consistent with the license and the original software license remains at the appropriate SPT office so that SPT may conduct accurate audits (and respond to external audits).

Unauthorised Access

Unauthorised access to SPT e-mail, internet, and computer resources is strictly prohibited. For example, Users are prohibited from accessing other Users' files or communications without any legitimate business purpose, regardless of the security designation assigned to a particular file or communication. Additionally, unauthorised use of diagnostics, vulnerability and hacking tools is strictly prohibited.

6. Mobile Devices

Laptops

It is the responsibility of each laptop user (asset owner) to take reasonable precautions to safeguard the security of the laptop and the information contained upon it. Each individual must ensure that the correct procedures are followed. This includes protecting it from physical hazards, including spilling liquids, not allowing unauthorised Users access to the machine and only using approved software.

In addition to the general Computing guidance, the following procedures must be adhered to at all times:

- When travelling use a carrying case, this will reduce the risk of accidental damage
- When travelling or working out of the office, keep your laptop with you at all times
- Store your laptop in a secure cabinet when not in use in an office environment
- Screensavers – as with Desktop PCs a password protected screen saver must be set as a means of protecting against casual security breaches
- Do not display sensitive information in a public place where the screen can be overlooked
- If a laptop is shared between staff, ensure that it is signed in and out at all times by the individual using it. At all times, there must be a nominated owner

Mobile Phones and Tablets

The following controls must be adhered to for any device containing SPT information:

- The device must be locked when not in use. The locking mechanism may be through PIN, password, passphrase, biometric control or pattern
- The device must automatically lock after a maximum of 5 minutes unless exception is granted by Digital Manager
- No apps other than from legitimate sources (iTunes Store, Google Play) are permitted unless exception is granted by the Digital Manager
- The device will be configured to allow remote wipe or reset of all data
- Any loss of a device must be reported to SPT's Digital Service Desk within 24 hours, and the device may be wiped
- Users must not uninstall any SPT configurations such as mobile device management apps

Teleworking/Home Working

Certain SPT staff members are permitted to work outside of the office in certain scenarios (refer to SPT's Guidelines for Working from Home). However, precautions must be taken to ensure this is being performed at an acceptable level of security.

The following precautions should be taken when working outside of the office:

- Connections should be made via the provided SPT VPN on any network
- Caution should be adopted when working in public spaces. Be aware of what is visible on your screen/people eavesdropping

- Documents containing personal, commercially sensitive or security related information should only be worked on in complete privacy
- Laptops should remain locked when not in use
- Laptops should only be used by the assigned owner or Digital administrator(s)
- If not securely stored, any removable media should remain on your person always, even when not at your laptop

Removable Media

Employees must take extreme care when using any removable media including but not limited to USB keys, CDs, DVDs, removable drives and tapes. Only SPT encrypted USB keys are to be used and available from the Digital Service Desk. Personnel are not permitted to attach portable memory sticks; hard drives or CD writers, to SPT IT equipment without authorisation from the Digital Service Desk or Digital Manager.

Information must not be stored on or transported on such devices at any time unless the device is encrypted to the required FIPS standard (Federal Information Processing Standard). If you are unsure whether any device does conform to this standard, ask the Digital department who will advise you.

Magnetic media that are to be posted shall be encrypted and sent in secure physical packaging. Sensitive information shall not be sent in standard post, but encrypted and sent with an approved secure courier.

Disposal of Removable Media

The Digital Service Desk should be given any CDs, DVDs, USB memory drives and any other removable media containing sensitive information securely erase or physically destroy. A registered electronic waste disposal organisation is used to support this activity. A certificate of destruction must be supplied by an approved disposal organisation and the certificate stored securely for audit and regulatory purposes.

7. Other Prohibited Activities

SPT e-mail, digital assets (computers, laptops, mobiles, etc) and internet resources must **not** be used to:

- knowingly propagate any virus, worm, Trojan horse, trap-door programme or malicious code
- 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
- transmit junk mail, chain letters, or spam (the same or substantially similar messages sent to a large number of recipients for commercial or other purposes unrelated to SPT) or pyramid schemes of any kind
- download, play, or execute games.
- run and/or solicit outside business ventures.
- transmit, retrieve or store any communication of a discriminatory or harassing nature or materials that are offensive, obscene, pornographic or sexually explicit
- transmit abusive, profane or offensive language
- negatively impact the confidentiality, integrity or availability of information
- store personal information which is not related to SPT business activities

Removal of Equipment from SPT Premises

No SPT computing equipment or system or equipment (other than laptops, mobile phones/tablets) may be removed from SPT premises without formal authorisation from the Data Protection Officer, Digital Services Team Leader or Digital Manager.

For specific requests to remove equipment from SPT premises, e.g. to an external training site or for short-term loan, a request must be raised to the Digital department via the SPT Service Desk and must be authorised by either the Data Protection Officer, Digital Services Team Leader or Digital Manager.

Confidentiality and SPT Intellectual Property

Users may not place, post, transmit, or otherwise disclose confidential, sensitive, or proprietary SPT information, or any private information relating to any individual SPT employees, contractors, or customers, to anyone outside of SPT by any means, at any time, or for any reason. Likewise, SPT's name, trademarks, service marks, logos, and other intellectual property may not be used outside the scope of a user's assigned employment duties without express advance authorisation from the Data Protection Officer. SPT intellectual property includes, and is not limited to, any and all works created and/or developed by SPT employees or created and/or developed on SPT premises.

8. Passwords and Security

All passwords and security used in connection with SPT e-mail, computers, internet resources and other digital assets are SPT property and must be made available to the Data Protection Officer or Digital Manager if required for legitimate purposes.

Password Selection and Use

Passwords are the first line of defence for our Digital systems and together with the user ID help to establish that people are who they claim to be. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers, systems and data.

A weak password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include singular words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Everyone must use strong passwords with a minimum standard of:

- At least twelve characters
- Be more complex than a single word (such passwords are easier for hackers to crack)

Good practice is to use a combination three-word non-related pass phrase with capitalisation and special characters. i.e. **$ChocolatePlaneHorse.**

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone (except the Data Protection Officer or Digital Manager if required for legitimate purposes)
- Never use the 'remember password' function
- Never write your passwords down or store them where they are open to theft
- Never store your passwords in a computer system without encryption
- Do not use any part of your username within the password
- Do not use the same password to access different SPT systems
- Do not use the same password for systems inside and outside of work

Password Allocation

Wherever possible users will be set up with a temporary password which will require the user to change it at first logon.

Frequency of Password Change

Passwords should be changed regularly so that, should an account become compromised, it cannot be used beyond a certain date. Whenever users believe that their password has become compromised or suspect someone has used their User ID and password; in either case it must be reported immediately as a potential security breach via the Security Incident Reporting Procedure (http://spt.intranet.uk/library/spt-data-protection/).

- Passwords must be changed every 180 days
- Cannot use any of last three passwords

Use of SPT Users Passwords

SPT users must understand that their use of passwords will not preclude access, monitoring, inspection, review, or disclosure by authorised SPT personnel. SPT may unilaterally assign or change passwords and personal codes. The security of SPT's technology resources is every user's responsibility. Users are required to take reasonable measures to protect the confidentiality of all passwords and to immediately report a suspected compromise of assigned passwords to the Digital Service Team.

Unauthorised Access

Unauthorised use or disclosure of user passwords, is strictly prohibited. For example, Users are prohibited from accessing other User' files or communications without any legitimate business purpose, regardless of the security designation assigned to a particular file or communication. Additionally, unauthorised use of diagnostics, vulnerability and hacking tools is strictly prohibited.

Misrepresentation of Identity

SPT e-mail, computer and internet resources may not be used to misrepresent, obscure, suppress, or replace one's identity or the origin of data or communications. For example, "spoofing" (i.e., constructing electronic communications to appear to be from someone else) is prohibited. Each user's name, e-mail address, organisational affiliation, time and date of transmission, and related information included with electronic communications (including postings) must always reflect the true originator, time, date, and place of origination, as well as the original message's true content.

9. Employment Termination / Return of Assets

Before each user's last day of employment, he or she must return or otherwise surrender possession of all SPT technology resources (including computers, mobile devices, software, computer peripherals, electronically stored data, diskettes and other data storage devices, keys, and written passwords) in his or her possession, custody, or control. Upon termination of employment, SPT will remove User access to SPT buildings, e-mail, computer systems and internet resources.

10. Failure to Comply with Procedures

Access to and use of SPT e-mail, technology and internet resources is for the sole purpose of undertaking the tasks required for SPT. Users who do not comply with or breach these procedures may result in access to e-mail computer and internet resources being suspended and may result in disciplinary action. If you discover a breach which impacts the confidentiality, integrity or availability of information then you must follow the Security Incident Reporting Procedure (http://spt.intranet.uk/library/spt-data-protection/). Any misuse of technology assets should be reported to the Service Desk Team on ext 3731.

11. Revision of Procedures

SPT may amend, revise, or depart from these procedures at any time, with or without notice to maintain the integrity of SPT systems and assets. Revisions will be notified to all staff and following consultation where appropriate with the recognised trade unions. These procedures do not constitute, and shall not be construed as an express or implied term of a contract of employment.

12. Other Policies and Procedures

Activities may also be covered by other SPT policies and procedures including *Digital and Cyber Security Procedures*, *Data Protection Policy* etc.