IT POLICY

1. Policy Statement

1.1. South Yorkshire Passenger Transport Executive (SYPTE) views IT services as valuable business tools. The organisation wishes to gain benefit from the use of IT services without subjecting itself and stakeholders to undue risks through security weaknesses or misuse.

1.2. IT services include all services which use information technology including but not limited to PCs and laptops, software, telephones (fixed and mobile), email and the Internet.

2. Detailed Policy Elements

2.1. Detailed policy elements specific to particular IT services are included as appendices to this policy. These are:

- Appendix A – Email
- Appendix B - Internet Access
- Appendix C - Security
- Appendix D - Telephony

3. Policy Elements

3.1. General Exclusions on Usage

a) No employee shall:

i) use, or allow any other person to use, SYPTE systems to access the systems of any other organisation or individual without their permission or in an unauthorised way.

ii) disclose any information to unauthorised parties outside of SYPTE which would allow those parties access to the organisation's own systems or those of its partners, suppliers, customers or employees.

iii) use, or allow any other person to use, SYPTE systems to gain access to store, modify or distribute material which could be considered to bring the name of the organisation into disrepute or is illegal in nature.

iv) use SYPTE's IT resources for personal monetary gain, nor for commercial purposes that are not directly related to SYPTE business.

v) transmit SYPTE owned information (which is not already in the public domain) to individuals or organisations except in the normal execution of their duties

b) No employee shall participate in any activities via IT services (including non-SYPTE services) which could reasonably be considered to bring the name of the organisation into disrepute. Such activity will not be tolerated.

c) No employee shall make or send calls or emails that are unsolicited or of an offensive nature, these will be considered as bringing the name of the organisation into disrepute. An unsolicited call or email is any that the recipient would not reasonably expect to receive from the originator.

d) No contract should be entered into that use or are for external/3rd party IT products or services, unless the Principal Secretary and Solicitor or nominee has given prior written approval and with the knowledge of the Head of I&T.

e) No IT system (including databases) shall be developed or procured through any means without the prior written approval of the Head of Information and Technology or nominated deputy.

f) A high standard of conduct is expected of employees using IT services. Defamation or harassment of colleagues or others using IT services is prohibited.

g) If an employee receives a telephone call or message through any IT service which they find offensive, they may inform the Helpdesk. In such circumstances do not delete any such message from any storage system unless instructed to do so. The Information & Technology Department and Human Resource Team will, where necessary, carry out an investigation before making any decision on the matter, and will use absolute discretion.

h) IT resources are not unlimited. Network bandwidth and storage capacity has finite limits, and all Users connected to the network have a responsibility to conserve these resources. As such, the User must not deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others. These acts include, but are not limited to unauthorised use of the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses.

i) Employees are required to return all business related IT equipment, records and documents in their possession if they leave the employment of SYPTE.

3.2. Personal Use and Responsibility

a) SYPTE's IT services are for business use. Occasional and reasonable personal use is permitted provided it is normally carried out in the employee's own time.

b) Through its monitoring systems the organisation has the ability to identify personal use, and reserves the right to raise invoices for the appropriate charges. The organisation retains the right, following disciplinary proceedings, to raise invoices for charges where misuse of the policy has occurred.

c) Where goods or services are purchased by an employee, for their own use, using the organisation's IT Services, then this is done at the employees own risk.

3.3. Systems Access

a) SYPTE will not tolerate the unauthorised use of IT systems or the information contained within them.

b) Employees must keep all passwords and security codes secure.

c) Employees will be held responsible for all activity using any IT system (including mobile phones and login accounts for computer services) to which they have been given access. Employees should take precautions to stop unauthorised use when away from their desks (including the locking of screens).

d) These rules are particularly important where the equipment is not attached directly to the Executive's network or not used on Executive premises, as in the use of laptops or PDAs at home or in public places.

e) Individuals with access to the organisation's IT systems and who are found to have:

i) Damaged the organisation's own computer systems, or those of another organisation

ii) attempted to access a system or information within a system whether controlled by the organisation or another organisation without the controlling organisations authority

iii) attempted to exceed the facilities or privileges granted to them, whether through deliberate or negligent action may be subject to SYPTE's Disciplinary procedures.

3.4. Representation of SYPTE

a) No user shall purport to, or allow any other person to purport to, represent the organisation except in areas where they have the authority to do so.

b) Any personal statements not directly connected with the business of SYPTE must contain a clear statement to the effect that "This is an individual view and not necessarily an expression of the views or policy of South Yorkshire Passenger Transport Executive".

3.5. Data Protection Act 1998

a) All electronic content is subject to the Data Protection Act 1998. Using any IT system to process personal data must only occur with the express permission of the person concerned. Under the terms of the Act, personal data includes any information about a living identifiable individual, including their name, address, phone number, email address and any other information about the individual. If employees include such information they are deemed to be "processing" personal data and must abide by the law. Please refer to Data Protection Act guidelines for further information.

b) If you need to send other people's personal details to a third party, then you must follow the procedure for the transfer of personal data which forms part of the organisation's data protection policies. These procedures can be found on the Intranet.

c) In the event of SYPTE receiving a Subject Data Access Request, under the Data Protection Act, the organisation retains the right to search IT systems for the requested information. Wherever possible employees will be informed that this will occur prior to the search taking place, this however may not always be possible, in which case employees will be notified after the search.

3.6. Monitoring Of Systems

a) The Information and Technology Department is responsible for the operation of any traffic, usage and connection monitoring systems which the organisation determines should be operated. Information from such systems may be passed to Management to enable decisions on investment to be made and an understanding of the usage patterns of the organisations IT systems to be gained.

b) Use of many IT systems which include telephones, email and Internet are subject to routine logging of destination and duration to enable system performance and monitoring of costs to take place. The detailed content of these logs is retained for a maximum of 3 years.

c) SYPTE routinely runs monitoring reports on all users of all IT Services to assist line managers and IT with the management of IT resources.

d) The organisation has, and will maintain, the ability to monitor specific individual usage of IT Services including storage, printing, internet and email services.

e) The organisation reserves the right to carry out audits of the use of any IT service at any time.

f) In the event that an employee is absent from work and unable to give timely authorisation for access to be granted, SYPTE retains the right to check IT services for business related correspondence when there is a justifiable business reason.

   i) Written permission for access to employee systems in these circumstances will be required from a Management Board member, prior to the employee's Line Manager or other nominee being able to access the relevant system. Access to the employee's system will be removed as soon as reasonably possible following the individuals return to work or notification that such access is no longer required.

g) Routine manual inspection of the content of electronic information will not take place. Manual inspection will only occur if there is good reason to believe that the employee's usage:

   i) contravenes criminal law,

   ii) contravenes his/her employment contract,

   iii) contravenes any policy of the Executive,

   iv) contravenes discrimination law,

   v) amounts to a civil wrong (such as defamation),

   vi) means aspects of this policy are being broken,

   vii) or is required to protect health and safety

   Employees will be informed before any manual inspection takes place if appropriate or possible, unless the search is subject to paragraph 3.6 h.

h) Should the organisation detect use of a system, or information obtained from any system, by its employees that could be deemed to appear to contravene United Kingdom or International law, the matter will be referred in the first instance to the Principal Solicitor and Secretary. The Principal Solicitor and Secretary will decide whether the matter should be referred to the Police or other official body without notifying the employees involved.

i) It is likely that any telephone call, email message or access of Internet sites is being logged or recorded by others as well as the organisation. The policies of other organisations will vary from those of SYPTE's. As a result there is no guarantee of safety, security or anonymity when using unsecured IT services or those external to this organisation.

3.7. <u>Software</u>

a) SYPTE is committed to using software for which it is properly licensed and will not accept the use of unlicensed software or more copies of software than it has licences.

b) All computer software must be purchased through the Information and Technology Department. No user may purchase software by any other means

c) Software must not be installed on any equipment unless carried out either by the Information and Technology Department or with the express written permission of the Head of Information and Technology or nominee.

d) There must be no transferring of software between computers without the express permission and involvement of the Information and Technology Department.

e) It is forbidden for employees to load and operate software obtained from the Internet, via email, magazine gifts or other sources including 'public domain', 'shareware', 'freeware' or 'evaluation' software without the prior written permission of the Head of Information and Technology or nominee. This will only be granted in the event of suitable testing having taken place and the organisation having or being able to obtain an acceptable licence for the software.

3.8. Copyright

a) Users may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licences that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a licence or download any material without first obtaining the express written permission of the organisation from the Head of Information and Technology or Principal Solicitor and Secretary or nominees as appropriate.

b) Copyright exists in all Ordnance Survey and other mapping material (including internet based services such as Google and Microsoft) the employee must ensure that an appropriate licence is in place for the intended use of a map. Advice on mapping licences should be sought from the Senior GIS Analyst. Under no circumstances should mapping of any form be posted on the Internet without authorisation of the Head of Information and Technology or nominee.

3.9. Other

a) Delivery of information using some IT services (e.g. external email or faxes) cannot be guaranteed, neither can the authenticity of the sender or recipient, therefore if the content of a message is confidential or time critical then the sender should ensure that the message has been delivered and the correct person has received it.

4. Equality and Diversity

4.1. The organisation recognises its responsibilities and legal obligations under the Equality Act and will endeavour to respond with reasonable modifications to IT equipment and services

4.2. Any member of staff having difficulties with the use of IT equipment and services due to physical disabilities, or potential difficulties, should in the first instance consult with his / her Line Manager to carry out an assessment who may then consult the Health & Safety Manager for a further assessment.

4.3. A number of alternatives and modifications to equipment are possible and can be made if the Health & Safety assessment advises so.

4.4. This Policy and all public facing systems are assessed for impact against the Equality and Diversity framework.

5. Links to Other Policies and Procedures

5.1. The Head of Information and Technology and the Head of Organisational Development will decide if there has been any infringement of the contents of any part of this policy, including the appendices of this policy, which may subsequently be subject to SYPTE's Disciplinary procedures.

5.2. This policy should be read in conjunction with the organisations other published policies and IT protocols.

6. Review

6.1. This policy will be reviewed annually. Feedback from staff and information gained from the monitoring of the policy will be used to improve the policy. Appropriate legislative changes will be incorporated as a matter of course.

6.2. Changes to this policy shall be communicated to all staff and contractors through the standard internal communications methods.

APPENDIX A – EMAIL

Email

1. *Disclaimer*

   1.1. *The ability for employees to send emails to individuals and other organisations using the Internet is a key business requirement. The provision of this service leads to the risk of unsolicited emails being received by an employee (commonly called spam). The organisation uses appropriate tools to stop as many of these emails as possible from reaching employee's email accounts, some of which may be offensive to some employees. These tools will be maintained to ensure the protection is as effective as possible. It is not however possible to stop all unsolicited emails from reaching employee's email accounts.*

2. General Exclusions on Usage

   2.1. Email should not be used to download or import software onto SYPTE's systems without the prior written permission from the Head of Information and Technology or nominee. This includes software and shareware available on the Internet that may be received by email even if it is apparently free.

   2.2. Connection to the Internet for the purposes of email will be through appropriate security systems, the configuration and performance of which will be the responsibility of the Information and Technology Department. Within SYPTE premises the connection of PCs to the Internet, except via appropriate security systems, is forbidden.

   2.3. Automatic forwarding of emails to non SYPTE email addresses is forbidden.

3. Personal Use and Responsibility

   3.1. SYPTE's IT systems and services are for business use. Occasional and reasonable personal use is permitted provided it is normally carried out in the employee's own time. Reasonable personal use of email and the internet should be kept to a minimum and together must not exceed 30 minutes per day. In the event that this will be exceeded or circumstances dictate that personal use is needed in normal working time, explicit consent from your line manager on each occasion is required.

4. Representation of SYPTE

   4.1. Employees will create and attach standard email signature to their email correspondence according to the specifications of the Organisational Development department's 'Style Guide'. For further clarification on this contact the I&T HelpDesk for instructions if necessary.

   4.2. Full company contact information will be attached automatically to all external emails stating the business address and other required details under the Business Names Act 1990.

   4.3. A footer will be attached to all external emails automatically. This footer gives details about the company, the appropriate confidentiality notice and disclaimer. The wording of this footer is as below:

   Confidentiality Notice: This email transmission may contain confidential or legally privileged information that is intended only for the individual or entity named in the email address. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or reliance upon the contents of this email is strictly prohibited.

If you have received this email transmission in error, please reply to the sender, so that SYPTE can arrange for proper delivery, and then please delete the message from your inbox. Thank you.

4.4. All personal statements not directly connected with the business of the organisation must contain a clear statement to the effect that:

This is an individual view and not necessarily an expression of the views or policy of South Yorkshire Passenger Transport Executive

Employees must include this text themselves when appropriate, as it will not be included automatically.

5. Monitoring of Emails

3.1 All emails received by the organisation from external sources will be passed through anti-virus software before it reaches an employee's account. As part of this process certain generic categories of email attachments (lists of which will be issued from time to time) will be automatically removed due to the risk of virus or other malicious software being imported in SYPTE's systems. If an employee is uncertain about the source or content of an email attachment then they should contact the Information and Technology Department before opening the attachment.

APPENDIX B – INTERNET

Internet

1. *Disclaimer*

   1.1. *Users are cautioned that many of the pages on the Internet include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an email address on the Internet may lead to receipt of unsolicited email containing offensive content. Users accessing the Internet do so at their own risk and the organisation is not responsible for material viewed or downloaded by users from the Internet.*

2. *General Exclusions on Usage*

   2.1. Employees deemed to be accessing or attempting to access inappropriate sites deliberately and for a time exceeding that associated with an innocuous search may lead to disciplinary action. Inappropriate sites are those that other employees may find intimidating, upsetting, embarrassing, humiliating or offensive.

   2.2. The Internet should not be used to download or import software onto the organisation's systems without the prior written permission from the Head of Information and Technology or nominee. This includes software and shareware available on the Internet even if it is apparently free, including but not limited to screen savers, games and other applications.

3. *Personal Use and Responsibility*

   3.1 SYPTE's IT services are for business use. Occasional and reasonable personal use is permitted provided it is normally carried out in the employee's own time. Reasonable personal use of email and the Internet should be kept to a minimum and together must not exceed 30 minutes per day. In the event that this will be exceeded or circumstances dictate that personal use is needed in normal working time, explicit consent from your line manager on each occasion is required.

4. *Internet Access*

   4.1 Connection to the Internet for any purpose will be through appropriate security systems, the configuration and performance of which will be the responsibility of the Information and Technology Department. The connection, within SYPTE premises, of PCs to the Internet not via appropriate security systems is forbidden.

   4.2 Connection of mobile devices to the internet when not on SYPTE's premises must be protected by the specified firewall, anti-virus and/or connectivity systems

   4.3 The organisation has the right to, and will utilise software that makes it possible to identify and block access to Internet sites, other services that use a disproportionate amount of the organisations Internet resources or where these sites are not directly related to its business.

   4.4 Access to Internet services, beyond the standard level of access, must be requested from the Head of Information and Technology or nominee. Requests should be through Organisational Development for new staff or otherwise by email or memo from the budget holder responsible for the work area in question, giving brief reasoning behind the request.

   4.5 Where such access can be granted within existing systems and there are no major technical barriers, such access will be granted subject to the employees agreeing to abide by this policy.

5. Excessive Use

5.1 The organisation's Internet connection(s) are not unlimited. Network bandwidth has finite limits, and all Users have a responsibility to conserve these resources. As such, the User must not carry out business processes that unfairly monopolise internet resources to the exclusion of others including uploading or downloading large files (through FTP or otherwise), accessing large amounts of streaming audio and/or video files, or otherwise creating unnecessary loads on Internet traffic without prior agreement from the Head of Information & Technology or nominated representative.

6 Information Security and Privacy

6.1 Standard internet based file sharing and distribution services should not be regarded as secure and should not normally be used for the distribution or transfer of organisation information.

6.2 If you need to send other people's personal details to someone else then you must follow the procedure for the transfer of personal data which forms part of the organisation's data protection policies. These procedures can be found on the Intranet.

6.3 If you need to distribute information to 3rd parties in bulk electronically then advice should be sought from the Head of Information & Technology or nominated representative.

APPENDIX C – SECURITY

Security

1. Physical Access

    1.1. Sensitive IT areas will be protected by locked doors which require a special key or security code to open, CCTV, or similar monitoring, may be used to enhance security of these areas. Only authorised personnel will have access to these areas.. All confidential and licensed material will be held in secure cabinets and only available to authorised people. These authorised people will be required to sign a log book when items are removed and returned.

2. Personal and Laptop Computer Security

    2.1. It is the responsibility of each user to take all reasonable precautions to safeguard the security of the computer and the information contained on it. This includes protecting it from physical hazards, including spilling liquids; not allowing unauthorised users access to the machine and only using approved software.

    2.2. Documents stored on laptop hard disks or the C: drive of a PC are not backed-up and cannot be recovered if deleted. In the event of theft the documents may be able to be viewed by unauthorised persons.

    2.3. The storage of documents on the fixed hard disks (C:\ drive) of PCs is prohibited. Storage of documents on a laptop C: drive or re-movable hard drives of PCs should be for as short a time as possible to minimise the risk of data loss.

    2.4. Users are reminded of their extra responsibilities when they are in possession of a laptop computer to use either on or away from SYPTE premises. Laptop computers, PDA's or similar devices must be secured when left unattended for any length of time and should not be left out unsecured on desks overnight.

    2.5. The Information and Technology Department will use appropriate tools, including encryption, to protect data in the event of loss of physical devices; this does not replace the need for users to ensure appropriate physical security precautions are taken.

    2.6. All Policy rules apply whether the laptop equipment is attached to SYPTE's network or not.

3. Network Security

    3.1. The transfer of confidential information over unprotected communication links will be restricted, whether within the organisation's private network or via the public network. There will be sufficient safeguards in place to prevent unauthorised persons from accessing the organisation's IT systems. Where there is a need to connect with the public or other network outside of the control of the organisation this will be via an appropriately configured "firewall" or virtual private network".

    3.2. A minimum level of security will be maintained across all computer systems, the required level of security and controls will be determined by the highest level of confidentiality of the information handled. Where data is replicated across different elements of the network, sufficient safeguards will be put in place to ensure that the information is kept in step.

4. USB Devices

4.1. The use of USB and other storage devices (including but not limited to Cameras , MP3 players and mobile phones) not supplied by SYPTE for the transfer of organisational or partners data is prohibited. These will normally have encryption enabled.

4.2. The use of non-SYPTE supplied storage devices is only allowable to enable a 3rd party to run a presentation or similar.

4.3. The charging of any personal equipment using USB ports of PC's or Laptops is prohibited to reduce the risk of virus and malware infection and loss of data.

5. Connection of Non- SYPTE IT equipment to the organisation's network

5.1. The normal method of exchanging information between the organisation and its suppliers or other bodies will be through Internet email. Direct connections to the organisation's mail systems will not be permitted.

5.2. Where automated exchanges of information are required (electronic data interchange; EDI), suitable EDI facilities must be built into the packages, products or database applications used. Responsibility for ensuring that such features are specified rests with the managers controlling the acquisition process for the software involved. The specification for these facilities must comply with the Electronic Government Interchange Framework (eGIF) standards.

5.3. Under normal circumstances, direct access to the organisation's IT systems by suppliers or other associated bodies will not be permitted. It is recognised, however, that where there are close relationships with suppliers involved with major parts of the organisation's business, such direct access may be required. In such cases the business case must be agreed between the requesting manager and the Head of Information and Technology. This must explicitly cover the provision and proof of adequate security, and the 3rd party access procedure must be followed

5.4. Connection of individuals or contractors PC's to the organisations networks by any method will only be allowed if prior agreement has been given by the Head of Information and Technology or nominee.

6. Passwords

6.1. The username and password given to employees, agents and suppliers to allow access to IT resources are for the use of the individual for whom the account is created. Passwords must never be shared with anyone, even someone from, or claiming to be from, the Information and Technology Department.

6.2. If there is a need to allow someone to access information you have on the computer systems then this can always be done by means other than password sharing. Contact the Helpdesk (ext. 2222) for assistance.

6.3. For further advice on passwords please read the Password Guidance Document issued separately.

7. Internet Security

7.1. Suitable controls are in place to prevent security breaches or other negative consequences, such as accessing inappropriate information. All information downloaded from the Internet will be automatically scanned for viruses, this will also include attachments which are received by external e-mail.

8. Mechanisms for reporting actual or suspected security incidents

8.1. All employees of SYPTE have a duty to report any actual, attempted or suspected breach of IT security, including loss of physical device such as laptop or USB device, as soon as practical.

8.2 Such reports should be passed to the IT Helpdesk, and suitable action will be taken.

APPENDIX D – TELEPHONY USAGE

Telephony Usage

1. Telephony Access

1.1. Connection to telephony services for any purpose will be through appropriate security and filtering systems, the configuration and performance of which will be the responsibility of the Information and Technology Department.

1.2. SYPTE has the right to, and will, utilise systems that makes it possible to identify and block access to specific phone numbers and types of telephony services.

2. Mobile Telephony Services

1.1 It is recognised that some employees are required to have access to mobile telephony services to enable effective operation of the business. The authority for issuing such services and any specific procedures relating to their use is subject to approval from the relevant budget holder and Management Board Attendee.

1.2 Attention is drawn to the document entitled 'Policy and Guidance – Mobile Phone Use In Cars'

1.3 A charge for personal use of these services will be made to the employee.

1.4 Use of all such services will be monitored on a regular and ongoing basis.

1.5 The equipment issued is the property of SYPTE; it should not be tampered with, or modified without prior written approval from the Head of Information Technology or nominee. For the avoidance of doubt this includes installing SYPTE SIM cards in personal phones and using personal SIM cards in SYPTE phones.

1.6 The Information and Technology Department will supply a phone suitable for the business requirement. A list of approved phones suitable for the organisations business requirements will be maintained by the Information and Technology Department. Any variation to this list will be with the specific approval of the Head of Information and Technology and will require a full business justification to be produced.

The document entitled *Guidance for Mobile Telephony Users* gives more guidance on the specific usage of mobile telephony services. (This document details charging methods for personal calls, security precautions to be taken, how to report faults etc.)

2 SYPTE Telephone Services in Non-Executive Premises

2.1 It is recognised that some employees are required to work from home. The installation of telephony equipment in people's houses is subject to approval from the Human Resources & Standards Committee and must be in line with the organisation's published homeworking procedure which can be found on the Intranet..

2.2 Installation of telephony equipment, which is to be owned or paid for by the organisation, in property not under the direct control of the organisation and outside the scope of homeworking is subject to approval from Management Board.

2.3 A charge for any personal or non-SYPTE use of these services may be made to the relevant party.

2.4 Use of all such services will be monitored on a regular and ongoing basis.

3 Monitoring Of Telephony Systems

3.1 The organisation records calls made to Traveline and associated services for training and quality management purposes. It is not the organisation's policy to monitor or record calls made to other services in such a way that the content of a given message is known, unless requested to do so by the Police or other such authorised authority.

4 Personal use and Responsibility

4.1 SYPTE's telephones are for business use. Occasional and reasonable personal use of the telephone is permitted in the following circumstances:

- In an employees duties as a primary carer;
- To make appointments for medical or personal health reasons;
- Other brief, important matters that has to be dealt with during standard business hours.

In the event that personal use is required for any other reason explicit consent from your line manager on each occasion is required.

.

For and on behalf of UNISON

---------- ----------

Chair, Branch Committee Date

For and on behalf of South Yorkshire Passenger Transport Executive

---------- ----------

Director General Date