PERSONNEL COMMITTEE MEETING – 6 JANUARY 2009

EXECUTIVE SUMMARY SHEET – PART I

Title of Report:
Use of the Council's ICT Facilities Policy

Author(s):
Corporate Head of Personnel

Purpose of Report:

To seek approval of the Use of the Council's ICT Facilities Policy and its introduction in January 2009.

Description of Decision:

Personnel Committee is requested to:

(i) approve the revised Use of the Council's ICT Facilities Policy.

Suggested reason(s) for Decision:
The Council currently provides employees access to various computing an telephone facilities in order that they can fulfil their work related responsibilities. The existing Policy does not allow employees to use these facilities for their personal use during their own time. In support of the Council's digital agenda, this Policy has not been reviewed.

Alternative options to be considered and recommended to be rejected:
There are no alternative options.

Is this a "Key Decision" as defined in the Constitution? No **Is it included in the Forward Plan?** No	**Relevant Review Committee:** Policy and Co-ordination Review

Personnel Committee

6 January 2009

Use of the Council's ICT Facilities Policy

Report of the Corporate Head of Personnel

1.0 Purpose of Report

1.1 This report seeks approval of the Use of the Council's ICT Facilities Policy and its introduction in January 2009.

2.0 Description of Decision

2.1 Personnel Committee is requested to:

(i) approve the revised Use of the Council's ICT Facilities Policy

3.0 Background

3.1 The Council currently provides employees access to various computing and telephone facilities in order that they can fulfil their work related responsibilities. The existing Policy does not allow employees to use these facilities for their personal use during their own time. In support of the council's digital agenda this Policy has now been reviewed. The revised Policy is summarised in paragraph 4 below and attached as Appendix 1 for consideration.

4.0 The Proposed Policy

4.1 The revised Policy has been developed to give clear guidance, standards and provisions on using the Council's ICT Facilities. ICT Facilities are constantly changing and developing. New technology and software is regularly introduced into the workplace. Therefore, it is important that this Policy is flexible enough to meet the demands of a dynamic environment.

4.2 The Policy applies to all ICT Facilities such as networks, computers, Blackberries, telephones and e-mail.

4.3 This policy does not apply to Members. Complimentary codes and protocols are issued to Members relating to the use of Council resources and equipment, use of Council ICT Facilities and use of Member websites.

4.4 It is proposed that the ICT Unit will supplement this policy by issuing guidance and instructions to individuals on the specific Facilities that have been issued to them for the purposes of their role. For example when a Blackberry is issued the associated guidance will include information on why the Facility has been issued to them and any more detailed security and operating instructions required. Furthermore it is also proposed that other related policies such as disciplinary and induction are reviewed and updated as appropriate.

4.5 The ICT Unit also intend to incorporate a Frequently Asked Questions Page on the Intranet to address common questions that are asked relating to the use of the Council's ICT Facilities and this Policy.

4.6 It is intended that following if it is approved, the Policy will be launched on 12th January 2009. On that date the ICT Unit will launch a new "pop-up" box that will replace the existing grey "pop-up" box that currently appears when people start their computer. The new "pop-up" box will be designed to be clear and concise. It will firmly place the onus on users of the Facilities to read the policy. By clicking on "ok" users will be accepting the terms of the Policy. The "pop-up" box will include a direct link that employees can use to access the Policy.

4.7 In addition it is proposed that the ICT Unit email all users so that on the 12th January 2009 they will have a message with a link to the Policy, advising that a new policy is in place and stating that as a user they must read and agree to comply with this Policy before using the Facilities.

4.8 Corporate Personnel and the ICT Unit have been developed jointly in consultation with officers from City Solicitors and Internal Audit. Internal and external research was conducted to develop the policy, including a review of Policies from other regional Councils.

Use of the Council's ICT Facilities

1 Policy Statement

1.1 The purpose of this Policy is to:

- Ensure compliance with all applicable laws relating to data protection, information security, freedom of information, human rights and the use of this Policy.

- Protect the Council and its employees from the risk of violation of the Council's policies, financial loss, loss of reputation or defamation; and

- Ensure that the Council's computing and telephone facilities ("the Facilities") are not used so as to cause harm or damage to any person or organisation, including the Council.

2 Introduction

2.1 The Internet is a valuable resource, particularly in terms of conducting research, obtaining information and keeping up-to-date with developments. There are many business and personal benefits associated with Internet usage, which this Council recognises and supports. However, it is important that the risks to individuals and the Council are minimised.

2.2 This policy aims to support the best use of Corporate Internet and Intranet resources and facilities safely and within the standards required by the Council and the Community it serves.

2.3 Sunderland City Council ("the Council") provides you as an Authorised User with access to various computing and telephone facilities ("the Facilities to allow you (a "user") to undertake the responsibilities and duties of your position and to improve internal and external communication.

2.4 The Council regards the integrity of the Facilities as central to the successful provision of services. You must read and agree to comply with this Policy before using the Facilities.

2.5 You must read and use this Policy in conjunction with other Council policies and procedures including but not limited to the Employees' Code of Conduct, Disciplinary Procedure, Harassment at Work, Anti Fraud and Corruption Policy and Data Handling Guidelines.

2.6 This is the Council's Policy on the use of the Facilities and it includes:

- your responsibilities and potential liability when using the Facilities;

- the monitoring policies adopted by the Council; and

- guidance on how to use the Facilities.

2.7 This policy applies to all users of the Facilities including employees and other workers including casual and agency workers, secondees and contractors.

2.8 This policy does not apply to Members. Complementary codes and protocols are applicable and issued to Members relating to the use of Council resources and equipment, use of Council ICT Facilities and use of Member websites. These codes and protocols are at Part 5 of the constitution.

2.9 This Policy applies to the use of the Facilities in respect of:

- local, inter-office, national and international, private or public networks (including the Internet and Intranet) and all systems and services accessed through those networks whether accessed from Council premises, your home or any other location;

- desktop, portable and mobile computers and applications (including but not limited to personal digital assistants (PDAs) and Blackberries);

- desk telephones and mobile telephones (including but not limited to the use of WAP services and SMS/MMS messages); and

- electronic mail and messaging services.

2.10 Compliance with this policy is mandatory for all users of the Facilities. The Council reserves the right to take disciplinary action against any user of the Facilities for failure to comply with this policy. Breach or breaches of this policy, including misuse of the Facilities, may amount to misconduct or gross misconduct and may lead to disciplinary action and the imposition of disciplinary sanctions up to and including dismissal, in accordance with the Council's Disciplinary Procedure.

2.11 Where it is thought that an illegal act may have been committed, the advice of the City Solicitor will be sought and dependent upon that advice the Police may be informed.

2.12 Users acknowledge that personal use is offered as a privilege of employment with the Council and not as of right. Personal use of the Internet and/or web based e-mail facilities (as detailed in this Policy) can be withdrawn by the Council at any time.

2.13 Users are reminded that the information held and managed in the Council Facilities is Council information. Whilst the Council is held responsible for the information it holds or owns, users can be found to be personally liable for a

breach or breaches of applicable law and regulation, including where acts or activities are contrary to the provisions of this Policy.

2.14 Any accidental breach or breaches of the policy must be notified to your line manager or the ICT Unit as a matter of utmost priority. You must also notify your line manager or the ICT Unit if you suspect any misuse of the Facilities.

2.15 From time to time the Council, through its authorised officers and other methods, may monitor, intercept or review your use of the Facilities to the extent permitted by the law as set out in Section 8. By using the Facilities you expressly consent to the monitoring, whether those Facilities are being used for work related purposes or personal purposes.

3 Computer Facilities - Use Of Computer Systems

3.1 Subject to anything to the contrary in this Policy the Facilities must be used only for carrying out the duties for which access to the Facilities was granted.

3.2 In order to maintain the confidentiality of information held on or transferred via the Facilities, security measures are in place and must be followed at all times. A log-on ID (user name) and password are required for access to the Council's ICT Facilities. Log-ins and passwords must not be shared. The Council reserves the right to override your password and obtain access to any part of the Facilities for monitoring, contingency or development purposes.

3.3 You are responsible for keeping your password secure. You must not disclose it to anyone, including colleagues.except as expressly authorised by your Line Manager or Head of Service. The ICT Unit may reset your password and request that you change it. The ICT Unit will never ask you to disclose your log-on password.

3.4 You are expressly prohibited from using the Facilities for the sending, receiving, printing or otherwise disseminating the information of the Council or its partners other than in the normal and proper course of carrying out your duties for the Council. This includes confidential information and all other information that is not already in the public domain. (See also Section 6.1).

3.5 In order to ensure proper use of the Facilities, you must adhere to the following practices:

- You must notify the ICT helpdesk if you believe that the anti-virus software on the equipment you are using is not working correctly.

- You must ensure that all removable media (memory sticks, CD, DVD, floppy disc and any other forms of media storage) is stored securely and if the removable media is to be transported between locations that adequate precautions are taken to protect it from loss or theft. If you are unsure about the precautions you should take, you must agree this with your manager.

- All removable media increase the risk of introducing a virus or other harmful software (malware) to the Council's network. Guidance must be sought from the ICT Unit before the contents are accessed or stored on the Council's network or hard drives. This information is published on the Intranet under "Data Handling Guidelines".

- Obvious passwords such as birthdays and spouse names must be avoided. The most secure passwords are random combinations of letters and numbers.

- If you become aware that your password is no longer secure you must change it immediately.

- When you are sending data or software to an external party by removable media always ensure that the device has been checked for viruses and "Data Handling Guidelines" available on the Intranet have been followed.

- All files must be stored on a network drive which is backed up regularly to avoid loss of information.

- Always log off the network before leaving your computer unattended.

- Always switch off your computer at the end of the working day.

- Only use the Sunderland City Council Wallpaper and screen saver with password protection enabled.

- Any Facility that is left unattended must be locked.

- Facilities must be shut down in a controlled way over night.

4 Software

4.1 Software piracy could expose both the Council and the user to allegations of intellectual property infringement. The Council is committed to following the terms of all software licences to which the Council is a contracting party. This means, in particular, that:

- software must not be installed onto any of the Council's computers unless this has been approved in advance by the ICT Unit. The ICT Unit will be responsible for establishing that the appropriate licence has been obtained, that the software is virus free and compatible with the Facilities.

- software must not be removed from any computer nor must it be copied or loaded on to any computer without the prior consent of the ICT Unit.

5 Laptop Computers

5.1 The use of a laptop creates additional problems especially in respect of potential breaches of confidentiality. When using a laptop you must also remember that:

- You are responsible for all equipment and software until you return it. You must take appropriate steps to ensure that the laptop remains secure at all times. For example, lock the laptop in the boot of your car rather than leave it on view.

- You are the only person authorised to use the equipment and software issued to you. Family and friends must not use this equipment and software. If, however, you are authorised to permit another Council employee, Member or other Council worker to use the equipment or software, you must ensure that they log-on using their own user name and password. You will remain responsible for the equipment and software and for ensuring their usage complies with the terms set out in this Policy.

- All data kept on the laptop must be backed up regularly in order to protect data against theft, mechanical failure or corruption. Documents stored in the 'My Documents' area on a laptop or PC are syncronised with documents stored on personal filestore on a server when connected to the corporate network. Documents stored on the personal filestore are automatically backed-up every night. Laptop users must connect to the corporate network on a regular basis to ensure that files are syncronised and backed-up.

- You must password protect confidential data on removable media or on the hard drive to protect against theft or loss. All laptop disks must be encrypted and an initial boot up password employed. Information is available on the corporate intranet on how to encrypt files and removable media.

- If you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the attention of the ICT Unit.

- Upon the request of the Council at any time, for any reason, you will immediately return any laptop, equipment and all software to the Council.

6 E-mail (Internal Or External Use)

6.1 E-mail is not a secure medium of communication – it can be intercepted and read. Do not use it to say anything you would not wish to be made public. If the information you are sending is data protected, confidential or otherwise sensitive material which should not be made public you should seek assistance from the ICT Unit on how the information can be secured. Appropriate security must be applied to information sent by e-mail. Particular care must be taken when the personal data of individuals is involved.

6.2 E-mail should be treated as any other documentation. If you would normally retain a certain document in hard copy you should apply a similar retention policy for the e-mail equivalent. If a statutory request to access information has been received it is an offence to destroy or modify that information.

6.3 When sending an e-mail message you must be aware that the recipient(s) may forward the e-mail message to others. Do not put anything in an e-mail message that you would not put on Council letter headed paper.

6.4 As with many other records, e-mail may be subject to disclosure in internal investigations or external legal investigations. Like all communications, you should not say anything that might appear inappropriate or that might be misinterpreted by a reader.

6.5 Users of the Facilities need to be aware that legally binding contracts can be formed by e-mail correspondence even if inadvertently and ensure that no contract is entered into unless the user is authorised to do so.

6.6 Your e-mail inbox should be checked at least daily. If you are unable to view your e-mails and you use e-mail as an external means of communication you must ensure that the autoreply service (out of office assistant) is used to inform the sender that you are unavailable. If you have any doubt as to how to use these Facilities please contact the ICT Unit. You must incorporate the following statement into the out of office message:

"If you are making a request for information under the Freedom of Information Act, please redirect your request to: freedom.information@sunderland.gov.uk. and it will be treated as received when it is received at that address."

6.7 You are not permitted to use the Council's e-mail Facilities or any sunderland.gov.uk address for personal use.

6.8 You are, however, permitted to use external web based e-mail Facilities for reasonable personal use within your own time i.e. break times, lunch times or before or after work. Where applicable you must be keyed or logged out of the Flexible Working Hours System. If you are unsure about when you are able to use the Internet for personal use, you must seek approval from your manager.

6.9 Furthermore, e-mails using external web based Facilities is only permitted provided that, such emails:

- do not contain information or data that could be considered to be obscene, racist, sexist, offensive, discriminatory, hurtful, inappropriate, derogatory, defamatory, harassing or bullying or in breach of legislation, and provided that such use is not part of a pyramid or chain letter; and

- are not used for the purpose of carrying out any business activity .

6.10 Viewing, displaying, storing (including data held in the computer's memory, local hard drive, network drive, e-mail system or other applications) or disseminating material via e-mail (including text and images) that could be considered to be obscene, racist, sexist, offensive, discriminatory, hurtful, inappropriate, derogatory, defamatory, harassing or bullying or promoting violence or illegal acts is strictly prohibited. The use of the Facilities for such activities is strictly prohibited and may result in criminal and/or civil liability. The legal focus in a harassment case is the impact the allegedly harassing material has on the person viewing it, not how the material is viewed by the person sending or displaying it.

7 Internet

7.1 The main purpose of providing Internet access is for Council business purposes, however appropriate personal use of the Internet within your own time is permitted. The Internet is a valuable resource and this Council recognises and supports the business and personal benefits associated with providing Internet access within the provisions set out below.

7.2 Use of the Internet and accessing web pages over the Internet is permitted. However, running third party applications over the internet, retrieving data over the Internet, FTP file transfers or access to news groups (unless authorised by the Council) is strictly prohibited. You are responsible for ensuring that you are the only person using your authorised Internet account and services.

7.3 Downloading any file from the Internet using the Facilities increases the risk of introducing viruses and malware to the Council's network. Guidance and approval must be sought from the ICT Unit prior to any such download.

7.4 Viewing, downloading, storing (including data held in the computer's memory, local hard drive, network drive, e-mail system or other applications) displaying or disseminating materials over the internet (including text and images) that could be considered to be obscene, racist, sexist, offensive, discriminatory, hurtful, inappropriate, derogatory, defamatory, harassing or bullying or promoting violence or illegal acts is strictly prohibited. The use of the Facilities for such activities is strictly prohibited and may result in criminal and or civil liability. The legal focus in a harassment case is the impact the allegedly harassing material has on the person viewing it, not how the material is viewed by the person sending or displaying it.

7.5 Posting information on the Internet, whether on a newsgroup, a chat room, blogs or e-mail is no different from publishing information in a newspaper. You must take care to ensure that if you do make a posting that it cannot be interpreted to be defamatory, discriminatory or harassing, otherwise you and the Council could face legal claims. You should also be aware that posting of information to criticise the Council, Members or Officers is a breach of the mutual trust and confidence implied into all employment contracts and may give rise to disciplinary action. This applies to postings accredited to an individual or made anonymously.

7.6 Users must note that activities over the Internet are subject to copyright, publishing, libel, data protection, software licensing and intellectual property rights legislation, and must comply with these requirements when using the facilities.

Personal Use of the Internet

7.7 Subject to the above you are authorised to use the Internet for personal use during your own time; i.e. break times, lunch times or before or after work. Where applicable you must be keyed or logged out of the Flexible Working Hours System. If you are unsure about when you are able to use the Internet for personal use, you must seek approval from your manager.

7.8 The Council's Internet access system records the access that each user makes through the Internet including the website accessed, the time spent on the site and the time/date of access. Access to this information is strictly controlled. The ICT Unit will only make reports of individual use available at the request of the HR Function or Internal Audit in the course of an investigation or at the request of the City Solicitor to support a police investigation.

7.9 As a user of these Facilities you agree and accept that any personal details you place on any Internet site(s) are placed at your sole risk. The same applies to personal transactions made using the facilities. You accept and acknowledge that the Council shall not be liable to the user for any losses, damages, claims, costs and expenses you incur as a result of disclosing personal details or information on an Internet site or entering into personal transactions using the Facilities. The Council recommends that you exercise caution and satisfy yourself that such disclosure is secure before disclosing personal details, such as credit card or banking details. You must be aware that personal details may also be stored on the Council's network servers or local devices and accept the associated risks.

7.10 Using the Internet for the purpose of trading or carrying out any business activity other than Council business is strictly prohibited.

7.11 As a user of the Facilities you are prohibited from entering into any personal transactions that involve the Council in any way, including for example, arranging the delivery of goods or items to a Council address or location.

7.12 When accessing the Internet for personal use, you must not download files or software under any circumstances. This includes any data, software, games, music, images and video files.

7.13 For the avoidance of doubt the matters set out above include use of WAP (wireless) facilities.

8 Monitoring Policy

8.1 The Council recognises the importance of an individual's rights to privacy and respects those rights. The Council must balance these rights against the requirement to protect others, ensure proper use of Council resources, and preserve the integrity and functionality of the Facilities. Use of information obtained from monitoring may be used by the Council in respect of enforcement of this Policy, including in disciplinary action.

8.2 The Council will from time to time monitor the Facilities. The principal reasons for this are to:

- detect any harassment, discrimination or other inappropriate behaviour by employees, ensuring compliance with contracts of employment and relevant policies applicable to employees and other users of the Facilities including, but not limited to Health and Safety at Work, Harassment at Work and Codes of Conduct.

- ensure compliance with this Policy;

- enforce and protect the integrity of the Facilities and any sensitive or confidential information belonging to or under the control of the Council;

- ensure compliance by users of the Facilities with all applicable laws (including the Data Protection Act 1998 and Freedom of Information Act 2000), Regulations and Guidelines and Codes of Practice published and in force from time to time; and

- monitor and protect the well-being of employees, Members and other users of the Facilities.

8.3 The Council may adopt at any time any one of a number of methods to monitor use of the Facilities. These may include:

- recording and logging of internal, inter-office and external telephone calls made or received by employees or other users using its telephone system (including where possible mobile telephones) in accordance with the Council's Call Recording Policy. Such recording may include details of length, date and content of calls. The Council's practice is only to record calls at the Customer Contact Centre at the Port of Sunderland. The Council will not record any other telephone calls unless it is legally required or authorised to do so.

- recording and logging the activities by individual users of the Facilities. This may include opening or sending e-mails and their attachments, monitoring Internet usage including time spent on the Internet and web sites visited.

- physical inspections of individual users computers, software and telephone messaging services.

- periodic monitoring of the Facilities including real time monitoring.

- archiving of any information obtained from the above including e-mails, telephone call logs and Internet downloads.

- E-mail sent from or to a sunderland.gov.uk address will be treated as Council information and monitored accordingly. Personal Internet e-mail will only be monitored in exceptional circumstances to the extent permitted by law and will require the explicit authorisation of the City Solicitor. It is noted again that personal use of the Council's email system is not permitted. Web based email is permitted within your own time, under the provisions within this Policy.

- The Facilities can be accessed from a number of locations including home working and places with wireless Internet access. As a user you must be aware that the ICT equipment monitors transactions from wherever the user accesses the Facilities.

8.4 The Council will not (unless required by law):

- allow third parties to monitor the Facilities; or

- disclose information obtained by such monitoring of the Facilities to a third party or third parties.

8.5 The Council may be prohibited by law from notifying individuals using the Facilities of a disclosure(s) to a third party or third parties.

9 General Guidance

9.1 Never leave any equipment or data (including customer data, laptops, computer equipment, mobile phones and PDAs) unattended on public transport, in public spaces or in an unattended vehicle.

9.2 Always consider all available methods of communication, particularly when dealing with confidential and sensitive information, for example a face-to-face meeting, the telephone, hand delivery and suitably addressed internal post.

9.3 When using e-mail or sending any form of written correspondence:

- Be careful what you write. Never forget that e-mail and written correspondence are not the same as conversation. They are a written record and can be duplicated at will.

- Use normal capitalisation and punctuation. Typing a message all in capital letters is the equivalent of shouting at the reader.

- Check your grammar and spelling; and

- Do not forget that e-mails and other forms of correspondence should maintain the high standards expected by the Council. Where applicable you should use formal headings and introductions such as "Dear…" and "Yours sincerely" etc.

9.5 Officers should use the asterisk function on the mobile telephone/Blackberry to ensure that they pay for all private personal calls, i.e. other than those made on Council business.

9.4 You should contact your manager or the ICT Unit if you are unclear about any part of this policy. The ICT Helpdesk telephone number is 553 5000.