Gateshead Council

www.gateshead.gov.uk

Standards, Procedures and Protocols

Governing the use of

Information and Communications Technology

(ICT) within Gateshead Council

25th April 2016

Table of Contents

1. INTRODUCTION 5

1.1 Who does this Policy apply to? 5
1.2 What is ICT equipment? 5

2. ACCESS TO COMPUTER SYSTEMS 7

2.1 Computer Access 7
2.2 ICT Nominated Representatives 7
2.3 Creation of new user accounts 7
2.4 Changes to levels of access 7
2.5 Access by non-employees 7
2.6 System Owners 8
2.7 Deletion of Accounts 8
2.8 Passwords 8
2.9 Choosing a Password 9
2.10 Keeping a Password Secure 10
2.11 If you forget your password 10
2.12 Unauthorised access 10

3. COMPUTER EQUIPMENT 11

3.1 Computer Usage 11
3.2 Procurement of hardware, software and systems (including externally hosted systems) 11
3.3 Procurement of computing equipment, hardware, software and services that support the core infrastructure (including desktop devices, laptops, printers and other peripheral devices connected to the Council's network). 11
3.4 Installation and removal of hardware and software 12
3.5 Windows security 12
3.6 Personal use of Council equipment 12
3.7 Use of personal equipment 13
3.8 Disposal of equipment 13
3.9 Use of laptop and handheld equipment 13
3.10 Portable storage devices 14
3.11 Housekeeping 16
3.12 Clear desk and screen policy 17
3.13 Environmental impact 17

4. SOFTWARE POLICY 18

4.1 Software Licence 18
4.2 Procurement of software 18
4.3 Software Installation 19
4.4 Screen Savers and Wallpaper 19

5. VIRUSES AND SPYWARE 20

5.1 Introduction 20
5.2 Anti-Virus Software 20
5.3 Hoax Viruses 21
5.4 Spyware 21
5.5 Anti Virus Precautions 22

6. INTERNET ACCESS 23

6.1 Introduction 23
6.2 General guidance 23
6.3 Specific requirements 23
6.4 Social Networking/Internet Forums 24
6.5 Copyright 24
6.6 Purchasing online 24

6.7 Council websites *24*
6.8 Personal Use of the Internet *24*
6.9 Personal use - What you CAN do *25*
6.10 Personal use - What you CAN NOT do *25*
6.11 Monitoring *25*

7. EMAIL **27**

7.1 Introduction *27*
7.2 General guidance *27*
7.3 When to use email *28*
7.4 What NOT to do when using email *28*
7.5 Writing Council Email messages *29*
7.6 Email format *29*
7.7 Subject Line *29*
7.8 Subject Matter and Tone *29*
7.9 Structure and Grammar *30*
7.10 Addressing *30*
7.11 Email signature *30*
7.12 Out of Office message *30*
7.13 Managing your mailbox *31*
7.14 Global Email *31*
7.15 Encryption and Digital Signatures *32*
7.16 Personal use of email *32*
7.17 Access to your mailbox by others *32*
7.18 Managing shared mailboxes and public folders *33*
7.19 Mailbox size *33*
7.20 When you leave the Council *33*
7.21 Attachments *33*
7.22 Virus scanning *33*
7.23 Spam email *34*
7.24 Disclaimer *34*
7.25 Council email addressing standard *35*
7.26 Monitoring of email *35*

8. INFORMATION SHARING **36**

9. TELECOMMUNICATIONS **38**

9.1 Telephone systems *38*
9.2 Fax machines *39*
9.3 Voice mail *40*
9.4 Mobile phones *40*
9.5 Mobile radios *41*

10. WIRELESS TECHNOLOGY **42**

11. REPROGRAPHIC EQUIPMENT **43**

11.1 Cameras *43*
11.2 Printers *43*
11.3 Photocopiers & Scanners *43*
11.4 Use of Recording Equipment *43*
11.5 Video Conferencing *43*
11.6 CCTV *44*

12. HOME / REMOTE WORKING **45**

13. PAYMENT CARD SECURITY **46**

14. INFORMATION CLASSIFICATION **47**

15. INCIDENT REPORTING **48**

16. MONITORING OF ACTIVITY **49**

16.1 Privacy and Confidentiality *49*

16.2 Internal Audit *49*
17. MISUSE **50**
18. RELEVANT LEGISLATION AND OTHER COUNCIL POLICIES **51**
19. POLICY REVIEW **52**
20. GLOSSARY **53**

1. *Introduction*

The use of Information and Communication Technology (ICT) is an indispensable part of work for many employees and helps the Council to provide effective and efficient services. To ensure that its full potential is realised, it is important that users understand their responsibilities in relation to the secure use of ICT resources and the information held within them.

This policy is designed to make all users of the Council's ICT systems aware of the security risks that are always present, and to protect the Council's information from all threats whether internal or external, deliberate or accidental.

This policy is based on the ISO 17799 & 27001 standards for information security, which contain comprehensive sets of security controls to improve the level of security within the organisation. The adoption of these controls provide a firm indication that the Council is taking "due care" of information which is one of the basic requirements of the Data Protection Act 1998.

1.1 Who does this Policy apply to?

This policy applies to any person who is granted access to Council ICT systems and equipment. Primarily this will be Council employees but also includes others that may be granted authorised access such as contractors, agency workers, temporary workers, work placements, employees of partner organisations, voluntary sector workers, external auditors, inspectors, visitors etc.

1.2 What is ICT equipment?

For the purposes of this policy, ICT equipment is defined as being any item of electronic equipment that is capable of storing or transmitting Council information. This includes, but is not limited to, technologies such as:

- Computers
- Email systems
- Internet access
- Telephones
- Mobile Phones
- Smart Phones
- Tablet Devices
- Fax machines
- Printers
- Scanners
- Photocopiers
- Mobile Radios
- CCTV
- Photographic equipment
- Audio recording
- Video recording
- Web cameras
- Video conferencing
- Networking equipment and cabling

It is recognised that developments in technology now allow a single device to be equipped with multiple areas of technology, for example a mobile phone can also be

used as a camera, a media player, a file storage system, an Internet and email access device etc. For the purposes of clarity, where a device is capable of utilising multiple areas of technology, each section of this policy relating to that area of technology will apply. If you are in any doubt about which sections are applicable you must ask before taking any action.

Failure to meet the requirements contained within this policy will present a risk to Council information and may result in action being taken under the Council's disciplinary process or the law (a list of relevant legislation is provided in section18 of this document).

2. *Access to Computer Systems*

2.1 Computer Access

Access to the Council's network is controlled by the use of authorised user accounts created within Windows Active Directory. You must not access or attempt to access any files, folders, logs, reports, messages, systems or information that has not been specifically authorised for you. If you are in any doubt please check with your line manager before attempting access.

2.2 ICT Nominated Representatives

Every Service in the Council has an ICT Nominated Representative. That is, a person authorised by their Service Director to request access to, and deletion from the Councils ICT systems for employees within their Service.

2.3 Creation of new user accounts

If you require access to the Council's computer network and ICT systems to carry out your duties please contact your nominated representative, who will complete and authorise a new user request form and pass it on to the relevant system owner e.g. ICT Services, Agresso Servicedesk, Idox, for creation.

2.4 Changes to levels of access

All changes to an employee's access privileges must be processed via the Service's nominated representative who will complete the relevant documentation and forward it to the relevant system owner.

2.5 Access by non-employees

It is recognised that occasionally there will be a need for suitably authorised people who are not Council employees to be granted access to Council systems in order to carry out their duties for example, inter-agency partnerships, joint working arrangements, commercial agreements or alternatively for inspectors, auditors, work placements etc.

Because these people are not employed by the Council they are not bound by the Councils code of conduct or security policy, therefore there are more risks associated with their access to the network. So that we can ensure the Councils data is protected, anyone wishing to arrange access for someone who is not employed by the Council must complete the relevant access request form and have it signed by the non-employee to state that they will adhere to the Council's policies. A contractor / visitor / temporary employee user access form can be obtained from the ICT Services Service Desk. The non-employee must not be given your password to share.

Where possible access for non-employees should be restricted to Read Only access.

2.6 System Owners

All Computer Systems (such as Agresso, Carefirst) have a system owner who is responsible for ensuring that adequate controls are in place to safeguard the information held within the system. Service Directors will ensure that a system owner is appointed for each Council system.

2.7 Deletion of Accounts

When an employee leaves the Council's employment, moves to a new role within the Council or is suspended pending disciplinary action, it is the responsibility of the relevant line manager to inform their nominated representative to arrange for the employee's network account and access to systems to be disabled or changed, as appropriate without delay.

Prior to leaving their Service or the authority employees should make every effort to pass on relevant information to their manager and ensure that any information required after their departure is accessible to the relevant people (this includes email messages and data stored in personal folders).

2.8 Passwords

Access to most Council computer systems is controlled by a "login" requiring a user-name and password. Anyone authorised to use a Council computer will be told personally the name and password to type in. This means that unauthorised users should not access the system.

In most cases the user-name will be a personal one and therefore the associated password will be a personal password.

Logging in with a personal user name and password:

- Opens up the personal access privileges the user has been authorised for in the system
- Provides the system with a personal identifier against which the actions taken by the user can be logged

If you are given a personal username and password to access a computer system, you must:

- Change it immediately if possible so that you become the only person who knows your password
- Keep your password confidential
- Do not tell your password to anyone else to allow them to access a computer system, even if you think they should have the same access rights to the system as you have, or have a similar job role
- Do not access a computer system using someone else's username and password for any purpose
- If you suspect that someone is using or attempting to use your username and password you must report it to your line manager immediately.

For some systems the user name and password may be group or generic ones if approved by the system owner. If this is the case you must not disclose the password to any employee or other person outside the authorised group.

Where other systems allow you to change your password you should do so, either in response to the system's prompt or at an interval defined by the system owner.

2.9 Choosing a Password

Choosing a secure password means that you reduce the chance of unauthorised persons accessing systems using your username. It is important that you choose a password that you can easily remember without writing it down.

When choosing a password you should select one that could not be easily guessed. Do not use information such as the name of your partner or child, your car registration number, date of birth or telephone number as your password. Computer programs have been developed by hackers to try and crack user's passwords. These programs often have access to dictionary lists so you should avoid using standard English and foreign words.

To keep password use effective as a control, passwords must be regularly changed. Microsoft Windows, which the Council uses to control access to many systems, will ask you to change your password when you first login as a new user. Commonly used words will not be allowed to be used in passwords. Your password must conform to the following format:

The password length must be at least 8 Characters including:
- A mix of alphanumeric characters
- At least 1 upper case letter

- Windows will prompt you to change your password every 90 days.

Also, your password:
- Must be different to the previous 20 passwords you've used
- Will lock out after 3 invalid password attempts

A good way of choosing a password is to create an abbreviation from a phrase you know or have thought of to create a "passphrase", such as:

"My hands have eight fingers and two thumbs", and use the initial letters to create the password **Mhh8fa2t**

"Jill had bacon and eggs for breakfast today" creates **Jhbae4bt**

"I went to Keswick for my holidays last August" creates **Iw2K4mhlA**

These are examples of good passphrases. They cannot be found in a dictionary, they contain a mix of upper and lower case letters, they contain at least one number, they are at least eight characters long and they should be easy to remember.

2.10 Keeping a Password Secure

- Never write your password down. The password that you choose should be easy for you to remember
- Do not let anyone watch as you type your password
- Never disclose your password to anyone, even if you think they should have the same access rights to a computer system as you have. No one else should ever need to know your personal password. Everyone who needs to have access will be given an account of their own.
- If you suspect that someone knows your password, change it immediately and if necessary inform your line manager.
- ICT Services will never ask you for your password. You should never need to divulge your password to anyone who asks you what your password is or tries to trick you into revealing it

2.11 If you forget your password

The Council uses password reset software called Specops to enable users to change or reset their Microsoft Windows password. You will need to enrol in the system prior to using this facility. It is installed on every desktop PC or it can be accessed by clicking on this URL: https://vmspecops.gateshead.pri/SpecopsPassword/Enrollment/Enroll.aspx. If you haven't already enrolled, please click here for instructions on setting it up.

If you do forget your password and have not enrolled in Specops then your line manager or nominated rep will need to log a call with the ICT Service Desk to confirm your identity and request them to reset your password.

2.12 Unauthorised access

With most of the Council's systems if you enter your username or password incorrectly three consecutive times the system will automatically disable your access and record the invalid attempts in a log file.

Log files are reviewed regularly to identify any possible attempts to breach access controls.

It is your responsibility as a user to help prevent illegal access attempts. To do this you should log off from your user account or lock your computer each time you move away from your computer and you should never disclose your password to anyone. If another person requires access to the same files as you they should contact their nominated representative to have their own access set up.

All users of the Council's systems must be aware that deliberate unauthorised use of passwords, attempts at unauthorised access to the network and systems, together with the unauthorised alteration of data are all offences under the Computer Misuse Act 1990.

3. *Computer Equipment*

3.1 Computer Usage

Authorised use of Council computers is permitted and encouraged where such use is for business purposes and supports the aims and objectives of the Council. Computer equipment is provided primarily for Council business purposes, however an element of personal use is allowed provided that the personal use does not have a negative impact on the operation of the Council.

If there is a requirement to use computer equipment away from the Council premises where it is normally located, the prior written approval of the line manager, or information asset owner whichever is appropriate, must be sought before any Council data or equipment is taken off site

3.2 Procurement of hardware, software and systems (including externally hosted systems)

All ICT business applications that are used for council business purposes must be procured through Corporate Procurement who will ensure that the security and technical implications are fully assessed by ICT Services before the procurement is completed.

There are additional risks that must be considered when procuring an externally hosted business application. At the beginning of the procurement, Services must produce an initial classification of the data that will be held on the system and this will be used in the procurement to determine whether the systems are appropriately secured, data protection requirements are being met, business continuity arrangements are adequate and data ownership at the end of the contract is clarified.

The completed data classification must be based on the classifications included in Section 14 of this document (page 46) and supplied to Corporate Procurement as part of the initial procurement request. It may also be appropriate, in line with the Information Commissioner's guidelines on system procurements, for Services to carry out a Privacy Impact Assessment (PIA). Services should consult the Councils Information Rights Officer, and ICT Services on this.
Depending on the outcome of the technical and security assessment and the PIA, Services may also be required to complete a full risk assessment and implementation plan before the procurement can be completed.

If you have a requirement for a new ICT business application or wish to procure an upgrade or additional modules for an existing business application you should contact Corporate Procurement in the first instance. Once the procurement of the business application is completed the order for the business application and all related services must be raised through ICT Services.

3.3 Procurement of computing equipment, hardware, software and services that support the core infrastructure (including desktop devices, laptops, printers and other peripheral devices connected to the Council's network).

All other computing equipment hardware, software and services that support the core infrastructure (including desktop devices, laptops, printers and other peripheral devices that are connected to the Council's network) and are used for Council business purposes must be procured via ICT Services, unless a separate Acceptable Use Policy exists for that device. ICT Services will ensure that only equipment and software meeting the Council's standards are procured and are therefore compatible

with existing software and hardware, comply with licensing legislation, are security asset tagged and are entered into the Council's ICT Asset Register.

If you have a requirement for new or additional computing equipment, hardware, software or services (including desktop devices, laptops, printers or any other peripheral device that is connected to the Council's network) you must contact the ICT Service Desk stating your requirements. ICT Services will in turn advise you what options are available and where applicable the costs associated with them. Whilst the procurement is carried out by ICT Services, your own Service is responsible for funding it. Therefore you must ensure that you have obtained your line managers approval and also budgetary approval from your Service Budget Holder prior to placing the request to ICT Services to purchase equipment.

3.4 Installation and removal of hardware and software

You must not install, attach, insert, connect, attempt to connect or remove any item of equipment to or from a council computer or the council network without prior authorisation from ICT Services. This includes all USB connected devices, with the exception of USB memory sticks (please see section below entitled Portable Storage Devices for further information on secure use of memory sticks). Similarly you must not install or attempt to install or remove software on any Council computer. Even if you are confident that you know how to install equipment or software you may not be aware of council specific settings that ensure they are correctly licensed, configured and do not conflict with each other.

3.5 Windows security

ICT Services install a Gateshead specific customised version of the Microsoft Windows operating system on all Council computers. A number of features that come with Windows are disabled as part of this customisation process to increase security and reduce the risk of compatibility problems. You may therefore find that you are unable to access certain applications or change settings in the same way that you can, for example, on a Windows home computer. In order to maintain this security and compatibility you must not attempt to access or make changes to the operating system or settings on Council computers.

3.6 Personal use of Council equipment

A limited amount of personal use of Council computing equipment is allowed in your own time, such as when you are keyed out of the flexi system, however it must not have a negative impact on the Council by:

- Interfering with the performance of your duties
- Taking priority over your work responsibilities
- Resulting in the Council incurring financial loss
- Bringing the Council into disrepute
- Being unlawful or contrary to Council policy or Code of Conduct

Council equipment may be used, for example, to prepare simple documents or spreadsheets on personal matters such as a letter to a bank or utility provider (please note that there is a separate section covering personal use of the Internet). Such personal documents should only be stored temporarily on the Council's computers whilst they are being prepared and should be deleted from the system after completion.

Personal documents may be printed and you will be charged for personal printing in line with a scale of charges. The printing of photographs and images is not allowed.

Equipment must not be used for your own private business purposes or for financial gain, nor must it be used to play games, music, videos etc.

3.7 Use of personal equipment

Personally owned ICT equipment must not be connected to the Council network or computers, unless otherwise covered by a separate acceptable usage policy. This is to prevent a number of potential problems occurring which may expose the Council to risks such as:

- Non-compliance with various standards the Council are required to adhere to such as PSN (Public Services Network), and PCI (Payment Card Industry Standard)
- Conflicts between versions of home and corporate software occurring when personal equipment is connected to Council equipment
- Non-compliance with software licensing agreements - it may be a breach of the licence agreement to install the necessary software or drivers for the equipment onto both a home and a Council computer, or to use the software for anything other than domestic use
- Uncertainty of ownership of data – For example, a personal camera used to take pictures for work purposes would create uncertainty over the legal owner of the images, and the images may not be able to be used for evidential purposes as they may not comply with PD0008 legal standard for admissibility of electronic documents. Additionally family and friends may then have access to the images
- Insurance claims for loss or damage – For example, if a personal camera being used to take pictures for work purposes is dropped and damaged it may not be covered by either Council or home insurance

ICT Services have a number of solutions available that will enable you to connect to the Council's network and work remotely. If equipment is required for work purposes away from the office this must be provided by ICT Services, please contact the ICT Service Desk and ICT Services will work with you to identify which solution will be most suited to your needs.

3.8 Disposal of equipment

All redundant items of computing equipment must be returned to ICT Services. This will allow ICT Services to update the ICT Asset Register and ensure that any associated ongoing support or licence costs are terminated. Services should also keep and update their own inventory of ICT assets. Where the licence permits, the software will be re-used or stored for future use. ICT Services will ensure that all Council data is securely removed, the hard disk degaused, the asset register updated and equipment disposed of in accordance with relevant legislation.

All redundant items of computer storage media such as CD's, DVDs, floppy discs, portable storage devices, tapes etc. must be securely destroyed or returned to ICT Services for secure disposal.

3.9 Use of laptop and handheld equipment

Laptops and handheld computing equipment offer a number of benefits over the more traditional desktop based computer in that they are portable and can be used off-site. However this increased flexibility also brings with it a number of risks, therefore the following controls must be adhered to.

- Wherever possible personally identifiable and sensitive data should not be stored on portable and handheld equipment. If it is essential that such data is

stored on this type of equipment you must seek approval from the information asset owner, in advance, before the equipment is taken off site. Additionally appropriate access controls must be applied to the equipment, such as password protection and encryption. Please contact the information asset assistant or information asset owner, for further guidance.

- Equipment and media taken off-site must not be left unattended in public places, including clients' homes.

- Equipment should not be left in vehicles unless absolutely necessary. Equipment left in vehicles must not be visible to passers-by, and wherever possible should be locked in the boot of the vehicle. Additionally all doors, windows and other means of access to the vehicle must be secured and locked and all keys removed to a place of safety. It must not be left in a vehicle overnight.

- Additional care should be taken if equipment needs to be left unattended in a hotel room, partner organisation's premises etc.

- Manufacturer's guidelines for protecting equipment should be observed at all times. Additionally, care should be taken to ensure that equipment is safeguarded from accidental damage, particularly whilst in transit.

- Care should be taken to ensure that display screens are not visible to passers-by.

- Council computer equipment must not be connected to any computer network other than the council's. Please contact ICT Services if you need to connect to a non-council network so that a secure solution can be arranged.

- Additional controls, required for frequent users of equipment off-site, and in particular home-workers, should be determined by a risk assessment carried out by your line manager and suitable controls applied, as the Information Asset Owner deems appropriate in line with the ICT Security Policy.

- Only authorised users may use Council equipment.

- You should be aware that information stored on laptops is not backed up unless the laptop is connected to the network and the files stored on a networked drive.

All council computers have anti-virus software installed on them. The version of anti-virus software on your computer is checked when you log on to the network and any updates required are automatically applied to ensure that the software is current and knows about the latest viruses. However, as some Council laptops may not connect regularly to the network the anti-virus software will therefore be out of date. If you are issued with a laptop you must ensure that you use it to log on to the network at least once a month. If you are unable to do this or are issued with a laptop and do not know when it last connected, you must bring it to ICT Services for a manual update to be applied before using it.

3.10 Portable storage devices

Portable storage devices can be physically very small but can store vast amounts of data. Being small, they are more easily lost or stolen. Loss or theft of a device which

contains any level of sensitive data could have serious consequences both for the Council and for the employee involved. The Information Commissioner can impose heavy financial penalties and custodial sentences for both organizations and the individuals responsible for security breaches involving personal data.

Examples of devices include but are not limited to: memory sticks, portable hard drives, cameras, mobile phones, personal digital assistants (PDAs), MP3 players, iPods, iPads etc, which typically connect to computers through a Universal Serial Bus (USB) port.

The appearance of a device type in the list above (which is not an exhaustive list) should not be taken as automatic endorsement that it is acceptable to use such a device for work-related data

Any transfer of data to any portable storage device must be approved by the Information Asset Owner (Service Director) or Information Asset Assistant.

The Information Asset Owner will determine if the level of data requires the use of an encrypted storage device.

The most common use of portable storage devices is the transfer to and from the device of data from and to the Council's network, often in connection with use away from the office (often therefore referred to as 'mobile data' purposes).

Except in the case of very specific examples such as disaster recovery plans and emergency contact lists held by senior managers, portable storage devices are short term, one-off 'overnight' solutions to 'mobile data' requirements and should not be used as a long-term data storage solution. For any longer term solutions such as more frequent or regular work away from the office environment, alternative solutions such as remote access to the Council's network must be considered.

Whether the portable storage device is used within or outside of the Council office, data loaded onto portable devices is not protected by the security which the Council network provides.

The types of data which need security are:

- Organisationally sensitive data (data which the Council does not publish).
- Personal data (anything that can be used to identify a living individual. It need not include the individual's name).

As well as security for existing data transferred from the Council network to storage devices, security may also be necessary for data created whilst away from the Council office and where results are stored on a portable device.

Council data stored on a portable storage device is owned by the Council regardless of who owns the device. Council policy on the use of Council data with these devices by employees is therefore as follows:

- Except in the case of the specific examples referred to above, portable storage devices are not intended for long-term storage of work data. If you have ANY Council data stored on any portable storage device it should be deleted as soon as the need to store it on the device is no longer there. Data should be transferred to the Council network at the earliest opportunity, and the data deleted from the portable storage device.

- You should NOT use your own personal portable devices for storing Council data which is personal data or organisationally sensitive data, even if your own device supports encryption.
- If your employment with the Council ends, any Council information that you have on any personal USB device of your own must be copied to the Council network prior to your leaving, and then deleted from your own device.
- If you wish to move or copy information, files, folders etc onto a portable storage device, you MUST obtain approval from your Information Asset Owner prior to doing so.
- Additionally you must maintain a list of files stored on the device which will assist should the device be lost or stolen.
- Line Managers, in conjunction with the Information Asset Owners, are responsible for ensuring employees are aware of their responsibilities in relation to the control and security of mobile data and for satisfying themselves that appropriate control and security measures are in place and will remain in place while the data is 'mobile'.
- Extreme care should be taken with all portable storage devices including encrypted Council devices due to their small physical size, they can hold large amounts of information and they can easily be lost or misplaced. Encryption of data on a device does not make loss or theft any more acceptable.
- You must report a lost, stolen or mislaid portable storage device immediately to:
  - your line manager
  - your Information Asset Owner
  - through the Incident Reporting email address, incidentreporting@gateshead.gov.uk.

Sometimes at seminars and presentations suppliers hand out complimentary empty portable storage devices to those who attend. If you receive one of these, then even though you may know the supplier, they should still be considered as an unknown or "untrusted" source. Prior to use on any Council device you should ensure the device is formatted to remove all files that might already be on it and might be virus-infected or contain spyware. For advice on how to do this please contact the ICT Services Service Desk.

Where contractors or other visitors bring their own portable storage devices into the Council and wish to connect them to Council devices (for example to give a presentation), this is acceptable providing the device they are connecting to has up to date ant-virus software installed (contact the ICT Services Service Desk if you need advice on how to check for this). Contractors and other visitors should however be supervised at all times whilst their portable storage device is connected to Council equipment.

3.11 Housekeeping

You must take care with food and drink near to computer equipment to ensure that the equipment is not damaged in any way should the food or drink be dropped or spilled.

You must not save data to the C: drive of your computer as this is not backed up and the data will be lost in the event of a failure.

Data and files should be saved on a shared network drive, but not the Z: personal drive, so that colleagues can access the information in your absence. Please refer to

the Councils Records Management policy in the Freedom of Information section on the Intranet for further information.

You must ensure that your file and folder permissions should be set to permit access only to employees that have a relevant business need. Please contact ICT Services for advice on how this should be done.

When using computer equipment you should position the screen so that information displayed on it cannot be seen by unauthorised personnel or through windows by passers-by.

3.12 Clear desk and screen policy

Offices and other Council premises can often provide easy opportunities for people to browse around and view documents or computer screens holding information not intended for them. Therefore you must take care to ensure that sensitive or personally identifiable information is not left on view or lying on desks whilst unattended.

All Council computers must be left with a clear screen whilst unattended. Computers will automatically lock after 10 minutes of inactivity to enforce this policy, however you should lock your screen whenever you leave your desk (using ctrl/alt/delete) for short periods of time, and log out if leaving your computer unattended for longer periods.

Sensitive or personally identifiable information should be cleared from printers and fax machines immediately, and should not be left on desks whilst unattended. Where possible, paper and computer media containing sensitive information should be stored in suitable locked cabinets when not in use, especially outside of office hours.

Computer printouts and any other documentation no longer required must be disposed of in a controlled and secure way which will prevent the data being disclosed to any person not authorised to receive it.

3.13 Environmental impact

If your computer is to be left unused for prolonged periods or overnight and at weekends it should be switched off to conserve energy.

You should only print documents when absolutely necessary, and where possible printing should be double sided.

Redundant equipment must be returned to ICT Services where it will be reutilised where possible, and at the end of its useful life disposed of with the minimum impact on the environment, in accordance with the relevant legislation.

4. *Software Policy*

4.1 Software Licence

All computer software must be used in accordance with its licence agreement Unless otherwise stated in an acceptable use Policy, all software will be delivered to, catalogued and held centrally by Corporate ICT Services to ensure compliance with FSSC-1, the Federation Against Software Theft (FAST) Standard for Software Compliance.

You must adhere to the following points in order to comply with software licence agreements:

- All software shall be used in accordance with its licence agreements.
- Unauthorised copies of any software must not be made under any circumstances.
- Any person illegally reproducing software can be subject to civil and criminal penalties, including fines and imprisonment. The Council does not condone illegal copying of software under any circumstances and anyone who makes, uses, or otherwise acquires unauthorised software may be subject to disciplinary action that could result in dismissal.
- Software must not be given or loaned to anyone including employees, clients, partner organisations, suppliers etc. without the prior approval of ICT Services.
- All software (including fonts, shareware and freeware) on Council-owned computers will be purchased through ICT Services, unless the Acceptable Use Policy states otherwise. In addition, only software that fulfils a required business need will be purchased.
- Deliberate unauthorised access to, copying, alteration, deletion or interference with computer programs and data or any action that interferes with the normal running of a computer system as intended by management is not allowed.
- If you suspect that there may be a misuse of software within the Council you must notify the Corporate ICT Manager or an appropriate Director/Service Director without undue delay.

4.2 Procurement of software

All software (including fonts, shareware and freeware) to be used on Council computers must be procured or obtained via Corporate ICT Services, unless the Acceptable Use Policy states otherwise. ICT Services will ensure that all software procured meets the Council's standards, is compatible with existing software and hardware, complies with licensing legislation and is entered into the Council's ICT Asset Register.

If you have a requirement for new or additional software you should contact the Corporate ICT Service Desk, stating your requirements. ICT Services will in turn advise you of the appropriate procurement route. Whilst the procurement of all software is carried out by ICT Services or Corporate Procurement, your own Service

may be responsible for funding it. Therefore you must ensure that you have obtained budgetary approval from your Service Budget Holder prior to placing the request to ICT Services to purchase software. For further guidance on software purchases please refer to assystNET FAQ 'Software Purchasing Advice'

4.3 Software Installation

Computer Software can only be installed or removed by Corporate ICT Services, or a person authorised by ICT Services to undertake the installation, unless the Acceptable Use Policy states otherwise. Under no circumstances is computer software to be installed or removed by any other person. This is to ensure that all software is correctly licensed and configured and does not cause conflict with hardware or other software already installed on your computer. Anyone who makes, uses, or otherwise acquires unauthorised software may be subject to disciplinary action that could result in dismissal.

4.4 Screen Savers and Wallpaper

To maintain a consistent corporate image and ensure the Council complies with software licensing legislation all Council computers have a standard screensaver and wallpaper installed on them. You must not change or attempt to change these.

The password-protected screensaver is invoked after 10 minutes of keyboard and mouse inactivity. It then requires you to enter a password to access the computer again. This minimises the risk of unauthorised access to your computer.

5. *Viruses and Spyware*

5.1 Introduction

Computer virus is a generic term used to describe a computer program written for the purpose of interrupting or affecting the normal operation of computers. The term virus is also often used to describe network worms, Trojan horses and other types of malicious software. Viruses are normally hidden from the computer user and can discretely copy themselves onto USB memory devices, or across computers and networks without the user's knowledge.

A virus program has to be run before it can infect your computer. Viruses do this by attaching themselves to other programs such as Outlook, Word or Excel or hide in code that is run automatically when you open certain types of files or carry out certain tasks. You might receive an infected file on a disk, in an email attachment, in a download from the Internet, or even by simply browsing a web site. Often the virus infection will occur without the user realising or noticing anything unusual happening.

Computer viruses are a threat to the operation of the Council. With the huge expansion in the use of the Internet and email, the spread of viruses has increased considerably in recent years and there are currently tens of thousands of different computer viruses in existence. Some viruses cause damage that is fairly minor and relatively easy to repair, however there are others where the damage to systems and networks can be so great that many weeks of work would be lost and major disruption to the operation of the Council could occur. Repairing and recovering systems from the effects of viruses can be extremely time consuming and may entail Council systems being unavailable for considerable periods of time.

The most common method of combating viruses is to employ anti-virus software that checks for the existence of viruses and acts accordingly when a virus is discovered.

5.2 Anti-Virus Software

The Council employs the latest virus-scanning software on all file servers, desktop computers and laptops. The software is configured in "on-access" mode, meaning that files are automatically scanned for viruses as they are accessed. All computers that are connected to the Council network have their anti-virus software updated automatically whenever it is necessary, often on a daily basis.

If a virus is discovered, the software is configured to automatically clean the file (i.e. remove the virus), send an alert to ICT Services and allow the computer to carry on working as normal.

The on-access facility means that you do not have to make special arrangements to have floppy disks, CDs, DVDs or USB memory sticks virus checked by ICT Services before they are used. They will be automatically scanned for viruses when you try to access files on them after inserting them into your computer. If they are found to be infected with a virus the system is configured to automatically try and remove the virus and allow you to carry on working as normal. Where this is not possible (CDs, DVDs or write-protected floppy disks cannot be cleaned) the system will deny you access to the infected file. In either case an alert window will appear on your computer screen informing you of the presence of the virus, what action has been taken and what further action if any, you must take. Additionally a further alert will be forwarded to ICT Services.

Because laptops are not permanently connected to the Council's computer network their anti-virus software quickly becomes out of date. To minimise the associated risks, laptop users need to take additional precautions to protect them from virus infection.

- Networked laptops need to be powered on and connected to the network at least once a month to ensure that they have the latest version of anti-virus software installed.
- Stand-alone laptops that never connect to the Councils' network need to be returned to ICT Services regularly so that the latest virus definitions can be added to ensure adequate protection against virus infection.

If you have a laptop computer and are unsure of its status you must contact ICT Services before using it.

An email gateway server scans all incoming email for viruses before they reach your Inbox. If an email addressed to you is received that is infected with a virus it will be cleaned at the gateway before it reaches you. Text will be added at the start of the email informing you that the virus has been removed and the email is safe to open.

You must not alter, or attempt to alter anti-virus software settings on any Council computer equipment.

5.3 Hoax Viruses

Email alerts are often sent around the Internet with warnings about the dire consequences of certain viruses, urging the recipient to forward the message on to all colleagues and friends immediately. These alerts may also ask the recipient to delete files from their computer or carry out some other remedial action. Very often these alerts are hoaxes designed to cause alarm, inconvenience and disruption to computer users.

If you receive a virus alert from any source other than ICT Services you should inform the ICT Service Desk. Do not forward a virus alert message to anyone else and do not delete any files unless advised to do so by the ICT Service Desk. If you are ever in any doubt contact the ICT Service Desk before you do anything.

ICT Services receive daily updates from the leading anti-virus software providers and should always be aware of the latest threats, both real and hoax.

ICT Services also provide information about the latest hoaxes and viruses in the Information Security Area of assystNET and on the Intranet.
(http://assystapp1:8080/assystnet/application/assystNET.jsp#;type=8;id=-1)

5.4 Spyware

Spyware comes in several different forms, all of which interfere with the normal running of a computer and/or collect and transmit potentially sensitive data without the user's knowledge.

The most noticeable effects of spyware are a slow computer, unwanted pop-ups or being redirected to websites that the user has not requested.

Many of these programs come bundled in with "free" software or search toolbars that add-on to the web browser and the user inadvertently agrees to their installation along with the toolbar. Some spyware simply monitors web browsing activity for marketing purposes however others are capable of performing unauthorised activity

such as collecting keystrokes, user information and even passwords. All forms of spyware increase the traffic loading on the Council's network unnecessarily.

The Council uses a standard web browser to access many of its critical applications and any changes to the configuration of the standard web browser may interfere with the correct operation of these applications. Additionally spyware increases the risk of sensitive council information being sent to unauthorised persons.

Therefore you must not install or attempt to install any web browser toolbars in line with the Council's software installation policy. If you suspect that your computer is infected with spyware please contact the ICT Service Desk.

5.5 Anti Virus Precautions

It must be emphasised that even the latest, up-to-date anti-virus software is by its very nature one step behind the very latest virus threats and can only detect what it knows about. When a new virus is discovered there is often a delay before the anti-virus software suppliers can write updates to their software in order to combat it. It is therefore important that you exercise caution at all times. In particular treat all email, especially those with attachments, as potentially suspicious. If you are ever in any doubt contact the ICT Service Desk before opening email or attachments.

6. *Internet Access*

6.1 Introduction

The Internet is a very powerful means of accessing and searching vast amounts of information quickly and easily. Use of the Internet by employees is permitted and encouraged where such use is suitable for business purposes and supports the aims and objectives of the Council. However employees should also verify the accuracy and validity of information published via the Internet before using it for Council purposes.

Access to the Internet also introduces a number of risks to both the Council and employees so all access to the internet is recorded by the web filtering system. The purpose of the Policy is to clearly define what is acceptable, what is not acceptable and what controls need to be adhered to when using Council equipment to access the Internet.

A limited amount of personal use of the Internet is also allowed provided that the personal use is reasonable and does not have a negative impact on the operation of the Council (see section 6.8 for more information).

All employees who have been granted access to the Council network will also by default be granted access to the Internet unless ICT Services are advised otherwise.

6.2 General guidance

The Council's Internet connection includes a "filtering" system that automatically blocks access to websites that are categorised as being inappropriate such as adult/sexually explicit, criminal activity, gambling, hacking, illegal drugs, intolerance and hate, tasteless and offensive, violence, weapons etc. Further categories will also be blocked because of the high risk of viruses and spyware associated with those types of websites, such as ringtones, mobile phone downloads, games etc.

However, due to the rapidly changing nature of the Internet it cannot be guaranteed that the filtering system or categorisation of websites is always 100% accurate. If you inadvertently access a website containing material that you consider to be inappropriate you must exit the site immediately and report it to the Corporate ICT Service Desk without undue delay. Similarly if you try to access a website that you consider to be legitimate and find that it is blocked, you should log the request to have it unblocked via the link provided on the blocking page.

6.3 Specific requirements

The following requirements apply to all use of the Internet, both for Council purposes and personal use using Council equipment:

- You must not intentionally access or attempt to access information or images that are obscene, sexually explicit, racist or defamatory or which depict violent or criminal acts or otherwise represent values that are contrary to Council policy
- All access to the Internet must be via a method approved in advance by ICT Services
- You must not access or attempt to access Internet based file sharing networks, such as Dropbox, Skydrive etc typically used for downloading, storing and sharing files, as the processes and procedures that would enable automatic checking of documents to prevent personal and\or

sensitive information being moved to these kinds of sites are not in place. If you are in any doubt you must contact ICT Services for advice before attempting to access any website.

6.4 Social Networking/Internet Forums

Internet forums can be an effective and efficient method of sharing information and best practice with peer groups and similar organisations. However users must be aware that any comments posted on a forum or social networking site may be visible to anyone in the world with an Internet connection. Users who join in these electronic discussions must conduct themselves in an honest and professional manner and ensure that their conduct does not bring the Council into disrepute. Users must not disclose confidential information and care must be taken to ensure that no personally identifiable information is disclosed about clients or service users. All views expressed must reflect the views of the Council and must be in accordance with the Council's Code of Conduct. This applies for both Council business use and personal use of the Internet.

6.5 Copyright

Much of what appears on the Internet is protected by copyright, which can include images and logos, as well as documents and information. The Copyright, Designs and Patents Act 1988 states that only the owner of the copyright is allowed to copy the information and any copying without permission, including electronic copying, is prohibited. Most web sites will include a statement informing you whether you need the website owner's consent before reproducing anything contained within the site.

6.6 Purchasing online

You must not acquire or procure any goods or services for Council business purposes directly via web sites or other Internet sources without first contacting Corporate Procurement for confirmation that you are complying with the latest procurement procedures.

6.7 Council websites

The Council maintains a number of websites that provide valuable information to residents, visitors and businesses on the Services the Council provides, as well as giving general information and news from around the borough. The websites also provide the mechanisms to allow Services to be accessed online. It is essential that all information published on any Council maintained website adheres to web standards. Requirements for new websites must be referred to the Web & Digital Manager for approval.

6.8 Personal Use of the Internet

Personal use of the Internet is allowed, however it must not have a negative impact on the Council by:

- Interfering with the performance of your duties
- Taking priority over your work responsibilities
- Resulting in the Council incurring financial loss
- Bringing the Council into disrepute
- Being unlawful or contrary to Council policy or Code of Conduct

If you have not been granted access to the Council Network as part of your job role you can gain access to the Internet for personal use via one of the Council's public Internet access facilities located at all libraries and the Civic Centre, which again must be done during your own time.

The employee must be clocked out if they are using the internet for personal use, and this must not interfere with the performance of their duties.

6.9 Personal use - What you CAN do

- Browse web pages (i.e. check the latest news, research a hobby, bank online)
- Buy goods and services online for personal use where a download to the computer is not required (i.e. shop online, book a flight or holiday, use an online auction site)
- Access browser based personal email systems (i.e. log on to Webmail to check personal email)
- Print information – a limited amount of personal printing is allowed and you will be charged for personal printing in accordance with the same mechanism as that for personal photocopying

6.10 Personal use - What you CAN NOT do

- Do not use it for gambling
- Do not use it for running a private business
- Do not use it to access payday loan sites
- Do not access Chat Rooms
- Do not use Instant Messaging or Web Messaging
- Do not download and / or upload software, images or files
- Do not download or play music or videos
- Do not download or play games
- Do not buy music, video etc if it requires a download
- Do not access streaming media (including radio and television)
- Do not create or update a personal website
- Do not have goods or services bought online delivered to your place of work
- Do not use your Council email address to subscribe to websites accessed for personal use
- Do not change settings on Council computers

The Council employs a number of measures to protect its computers from viruses and spyware etc. however no guarantee can be given that your personal details, bank and / or credit card details are secure. If you choose to enter personal details or buy online it is done so at your own risk.

You should note that whilst every effort will be made, there is no guarantee of availability of Internet access or of specific web sites for personal use.

It is important to note that no technical support will be given to resolve problems experienced when viewing any website that is not Council business related.

6.11 Monitoring

All access to the Internet is logged automatically by software that records the username of the employee, the websites visited, the dates and times of the visits, and the amount of time spent at each site. This applies to both personal and Council business use of the Internet.

Management are able to access detailed reports of sites visited by employees for both personal use and Council business use. Such reporting is not provided on a set

basis but is available to managers in the normal course of an investigation, or on suspicion of inappropriate or prolonged use of the Internet by an employee.

The impact of allowing personal use of the Internet and the effect it has on the Council network and Internet connection will be monitored regularly and it may be withdrawn if it is deemed to be having a detrimental effect to Council business.

7. *Email*

7.1 Introduction

Email is increasingly being used as one of the primary tools for internal and external communication. When used correctly email brings with it many advantages:

- It is a fast and inexpensive way of delivering messages and documents
- Information can be shared quickly and consistently between large numbers of people
- It can remove the need to print and distribute information by conventional means
- It provides a record of communication between sender and recipient

However, the use of email also introduces a number of risks to both the Council and employees, and the purpose of this policy is to clearly define what is acceptable, what is not acceptable and what controls you need to adhere to when using the Council email system in order to minimise those risks.

Use of email by employees is permitted and encouraged where such use is suitable for business purposes and supports the aims and objectives of the Council. A limited, reasonable amount of personal use of email is also allowed provided that the personal use does not have a negative impact on the operation of the Council.

Whilst this policy is primarily concerned with access to the Council's Gateshead.gov.uk email domain, the same principles apply to any email system (whether Council owned or not) used during the course of, or as a result of, your duties.

7.2 General guidance

Whilst email may often appear to be an informal method of communication you should remember that it has the permanence of written communication, and as such you must ensure that it meets the same standards as other published documents.

All email and attachments sent and received on Council equipment (including personal email) are owned by the Council. Therefore when using email as a means of communication you must keep in mind that:

- **All** emails are potentially subject to disclosure under the Freedom of Information Act
- Emails may be produced in court in the same manner as any other Council document
- Email communications, both internally and externally, cannot be guaranteed to be private or secure. Nor can they be guaranteed to arrive at their destination either on time or at all
- Advice given by email has the same legal effect as that given in any written format
- Once you have sent an email you have no control over who the recipient may then forward it on to, either intentionally or accidentally
- The impersonal nature of email messages can mean that it is easier to cause offence than when speaking and attempts at humour can easily be misinterpreted
- All emails are archived and a copy is retained by the Council for a minimum period of 6 months, including those that you have deleted from your mailbox

- You must not keep emails that are construed as business records in email folders. These emails should be saved on a shared drive in accordance with the Council's Records Management Policy.

7.3 When to use email

Email is not always the best way to communicate information. Messages can often be misunderstood and the volume of messages people receive can prohibit a meaningful reply as a result of email overload.

It is the responsibility of the person sending an email message to decide whether it is the most appropriate method of communicating. This decision should be based on a number of factors including:

The subject matter - you should consider the nature and sensitivity of the subject matter, and whether it would be more appropriate to communicate it in a different way. It is also important to remember that the privacy and confidentiality of messages sent via email cannot be guaranteed so care needs to be taken particularly when the subject matter is of a personal or sensitive nature. Additionally you should not use email to avoid a difficult face-to-face communication.

The recipient's location - there are times when email might not be the most appropriate way of communicating to for example, a colleague in the same office where speaking to them face to face might be more productive, particularly if they receive large volumes of email.

The speed of response - although email messages can be sent and delivered quickly there is no guarantee that the message will be read or acted upon immediately. Where an immediate action or response is required it may be better to speak to the person directly and send email confirmation if it is deemed to be necessary.

7.4 What NOT to do when using email

When using the Council's email system any behaviour or comments that are not permitted in the spoken or paper environment are also not permitted in email messages. Additionally:

- Do not send or forward email that could be construed as obscene, sexually explicit, racist, defamatory, abusive, harassing or which describes violent or criminal acts or otherwise represents values or opinions that are contrary to Council policy. If you receive email of this nature you should inform your line manager immediately
- Do not send unsolicited bulk email or Spam
- Do not forward chain mail or jokes
- Do not use email to send frivolous messages or gossip
- Do not forward messages unnecessarily
- Do not read, delete, copy or modify the contents of any mailbox other than your own without prior authorisation in writing from your Service Director, unless you have been delegated authority to that mailbox by the mailbox owner
- Do not generate email in such a way that it appears to have been sent from someone else
- Do not conduct any business other than that of the Council via email
- Do not enter into any commitment on behalf of the Council unless explicitly authorised to do so

- Do not register for automated alerts or subscription services unless there is a valid business reason for doing so
- Do not use a personal email account for Council business purposes
- Do not send information of a sensitive or confidential nature to any non council email account, without contacting ICT Services for access to the secure email facility provided by ICT Services. If you need to access the Council's email system from home please contact ICT Services who will arrange for secure access to be set up, subject to your line manager's authorisation.
- Use a Council email address to subscribe to websites accessed for personal use

7.5 Writing Council Email messages

Email messages are often treated as a form of informal communication even when they are used to communicate business decisions. It is important that the same care and attention is taken when composing an email message as that taken for a formal letter or an internal memo. If not there is a risk that the intended message will not be understood or acted upon in the appropriate way. This applies equally to both internal and external email communication. Therefore the following email etiquette should be adhered to:

7.6 Email format

- The default mail format should always be used to maintain a consistent corporate style
- Decorative graphics and icons should not be used as they can significantly increase the size of an email
- Do not automatically use Delivery and Read Receipt options, only use them when absolutely essential as they create unnecessary traffic on the Council's email system
- Be aware that some email systems might have difficulties with attachments and many systems limit the size of attachments to 2Mb. If you are unsure how to check the size of an attachment please contact the ICT Service Desk for further advice

7.7 Subject Line

- Ensure the subject line gives a clear indication of the content of the message
- Indicate if the subject matter is sensitive
- Do not include personally identifiable or sensitive information in the subject line as this is shown even in encrypted emails

7.8 Subject Matter and Tone

- Greet people by name at the beginning of an email message
- Ensure that the purpose and content of the email message is clearly explained
- Include a signature with your contact details
- Ensure your signature is in accordance with the corporate standard
- Ensure that the email is polite and courteous
- The tone of an email message should reflect the nature of the communication
- Make a clear distinction between fact and opinion
- Proof read messages before they are sent to check for errors
- Try to limit email messages to one subject per message
- Include the original email message when sending a reply to provide a context

- Where the subject of a string of email messages has significantly changed start a new email message, copying relevant sections from the previous string of email messages
- Ensure email messages are not unnecessarily long
- Ensure that attachments are not longer versions of emails
- Summarise the content of attachments in the main body of the email message

7.9 Structure and Grammar

- Try to use plain English
- Use Arial or Calibra 10 point as the font
- Check the spelling within the email message before sending
- Use paragraphs to structure information
- Put important information at the beginning of the email message
- Avoid using abbreviations
- Avoid using CAPITALS throughout
- Try not to over-use bold text

7.10 Addressing

- Distribute email message only to the people who need to know the information
- Using “Reply to All” will send the reply to everyone included in the original email. Think carefully before using “Reply to All” as it is unlikely that everyone included will need to know your reply
- Use the “To” field for people who are required to take further action and the “Cc” field for people who are included for information only.
- Think carefully about who should be included in the “Cc” field
- Ensure that the correct address is selected
- Use Bcc if the recipient list should not be disclosed

7.11 Email signature

To maintain a professional and consistent image an email signature should be used in line with the format detailed below:

Sarah Brown
Senior Clerk
Financial Services
Gateshead Council
Civic Centre, Regent Street, Gateshead, NE8 1HH

Phone: 0191 433 3000
Fax: 0191 433 3001
Email: SarahBrown@gateshead.gov.uk
www.gateshead.gov.uk

In the interests of the environment, only print this email if absolutely necessary.

7.12 Out of Office message

If you know you are going to be out of the office for a period of time and therefore unable to respond to email messages, you should set up an “out of office” message on your mailbox. The message should be professional, to the point and include detail of who to contact in your absence for both operational matters and freedom of information requests. If your absence is unplanned your line manager should arrange for the message to be added on your behalf by contacting ICT Services. The format for the out of office message is outlined below:

I am out of the office until Monday 4th September. In my absence please contact Sam Khan by email at SamKhan@gateshead.gov.uk or by telephone on 0191 433 3000.

If you are making a request for information under freedom of information or data protection legislation, please direct your request to LucyCarter@gateshead.gov.uk. If it is not redirected, your message will be treated as being received on the date of my return.

Regards

Sarah Brown
Senior Clerk

7.13 Managing your mailbox

Managing an email mailbox effectively can appear to be a difficult task, especially if the volume of email messages received is regularly of a large quantity. Managing an email mailbox should not be about following rigid guidelines, it is about following a methodology that works best for you which ensures that business records are managed in accordance with the Council's Records Management Policy (available on the Intranet).

There are a number of approaches that might aid the management of email messages such as:

- Setting up delegated access to your mailbox to allow a colleague to action messages in your absence
- Checking your mailbox regularly. If your job role does not allow you to do this you should either have email redirected to a colleague or grant access to a colleague so that they can take action on incoming email in your absence
- Allocating sufficient time each day or week to read through and action email messages
- Prioritising which email messages need to be dealt with first
- Looking at the sender and the title to gauge the importance of the message
- Noting where you have been "Cc'd" into email messages. These messages are often only for informational purposes and do not require immediate / any action
- Setting rules for incoming messages so they can automatically be put into folders
- Using folders to group email messages of a similar nature or subject together so they can be dealt with consecutively
- Deleting email messages that are kept elsewhere as records
- Deleting email messages that are no longer required for reference purposes from the Inbox and Sent Items
- Internal emails within the same Service area should, where possible, use pointers or shortcuts to documents rather than attaching the document to the email

7.14 Global Email

Although email is often considered to be a good way of disseminating information to large groups you should note that the ability to send a "global" email to everyone in the Council is restricted. You should also note that not all Council employees have access to email and therefore other methods of communication should be used to ensure that they also receive important information in a timely manner.

If a message needs to be conveyed to all computer users the message should ideally be placed on the Intranet or added to the weekly Council Info Bulletin. The Intranet contains further information on the procedures for this. Only email messages that are considered to be of immediate interest to the majority of computer users will be sent to everyone outside of the Council Info Bulletin process.

7.15 Encryption and Digital Signatures

If you need to send information of a personally identifiable or sensitive nature to an external recipient, it must be encrypted and where applicable digitally signed. You should note that password protecting a Word document or Excel spreadsheet is not considered to be a secure method of safeguarding data and should not be used to transmit sensitive or confidential data. Please contact ICT Services for further information regarding encryption and digital signatures.

7.16 Personal use of email

Personal use of email is allowed, however it must not:

- Interfere with the performance of your duties
- Take priority over your work responsibilities
- Result in the Council incurring expense
- Have a negative impact on the Council
- Be unlawful or contrary to the Council's Code of Conduct
- Wherever possible personal use of the email system should take place outside work hours, for example during lunch breaks.
- The amount of work time taken up by personal email must be kept to a minimum.
- This applies to incoming as well as outgoing personal email.

It is important to note that the rules governing business use of email are also applicable to all personal use of email.

You should create a folder named "Personal" within Outlook and move any email that you send or receive that is of a personal nature, and not in any way related to Council business, into this folder. You can automate this process by setting up a filter so that email to and from known personal contacts (such as family members) is routed directly into your Personal folder and not your Inbox. Additionally you should ensure the word "Personal" is in the subject line of any personal email you send or receive.

Email stored in the Personal folder will not ordinarily be accessed by others (see section below). Email relating to Council business must **not** be stored in the Personal folder.

7.17 Access to your mailbox by others

There may be occasions when it is necessary for your line manager or a colleague to access email messages in your mailbox. Typically this will be for business continuity reasons if you are away from the office for an extended period, for example away on business, on leave or absent through sickness. Additionally, access to your mailbox may be granted to action:

- Subject access requests under the Data Protection Act
- Freedom of Information requests
- Evidence in legal proceedings
- Evidence in a criminal investigation
- Evidence in support of disciplinary action

It is less likely that this procedure will need to be followed if email records are managed in accordance with the Records Management Policy, for example by storing them on a shared drive.

Email located in the folder marked as “Personal” will not ordinarily be accessed, however access may be granted to others as part of an investigation, or on suspicion of inappropriate or excessive use of email by an employee.

7.18 Managing shared mailboxes and public folders

All shared mailboxes and public folders have an owner who is identified when the mailbox is requested. The sections of this email policy relating to personal mailboxes should be adhered to when managing shared email mailboxes. Additional rules should also be in place relating to when to delete an email message from the mailbox and how to identify an email message as having been answered. It is the responsibility of the mailbox owner to ensure that there are specific rules relating to the management of shared mailboxes, and it is the responsibility of all employees with access to shared mailboxes to abide by those rules.

7.19 Mailbox size

Mailboxes on the Council’s email system are configured with a storage limit of 300Mb. This should hold approximately 200,000 typical email messages, although if your emails are large or you store a lot of attachments then this figure will be reduced. As your mailbox approaches the storage limit you will get a warning message. Managing your mailbox in accordance with the Council’s Records Management Policy should prevent this from occurring, however if your mailbox does reach its limit then you must save any email you need to retain elsewhere (i.e. shared storage areas) paying particular attention to email with attachments, delete any email no longer required and finally empty the “Deleted Items” folder.

7.20 When you leave the Council

When you leave the Council’s employment your mailbox will be disabled to prevent anyone from sending you further email. Access to your mailbox will be granted to a colleague who will process any outstanding actions, and after a period of three months the mailbox will be deleted from the Council’s system.

7.21 Attachments

There are increased security risks associated with email attachments, therefore certain file types are prevented from being sent and received on the Council’s email system, for example .exe, .bat, .com, .mp3, .scr etc.

Where possible you should avoid using these file types, however should you have a business need to have an attachment of this type sent or received then please contact the ICT Service Desk who will, where possible, arrange for that email to be transmitted.

Additionally, email with attachments larger than 10Mb will be blocked. You should also note that external organisations may also have attachment size limits on their email systems, and it is not unusual for this limit to be as low as 2Mb. One method of preventing problems is by having the attachment zipped or compressed. Please contact the ICT Service Desk for further details of how to do this.

7.22 Virus scanning

An email gateway server scans all incoming email for viruses before they reach your Inbox. If an email addressed to you is received that is infected with a known virus it will be cleaned at the gateway before it reaches you. Text will be added at the start of

the email informing you that the virus has been removed and the email is safe to open.

It must be emphasised however that even the latest, up-to-date anti-virus software is by its very nature one step behind the very latest virus threats and can only detect what it knows about. When a new virus is discovered there is often a delay before the anti-virus software suppliers can write updates to their software in order to combat it. It is therefore important that you exercise caution at all times. In particular treat all email, especially those with attachments, as potentially suspicious. If you are ever in any doubt contact the ICT Service Desk before opening email or attachments.

7.23 Spam email

Junk email or Spam is widely acknowledged as being a significant problem across the Internet. Spam is often annoying and disruptive however it can also potentially be dangerous to your computer and to your privacy.

The council's email system blocks more than two million Spam messages from reaching employees every month. Given the large volume involved, there is always the possibility of the occasional Spam email slipping through the net and reaching your Inbox.

It is important that you remain vigilant whenever you receive unsolicited email. This is particularly important if the email purports to be from a bank or building society asking you to confirm your banking or personal details. Fraudsters regularly send out emails that look like they come from banks (or other trusted organisations) and contain links to fake websites, which also resemble the real thing. Banks will never send you an email asking you to disclose PIN numbers, passwords or other personal information or which link to a page that asks you for this kind of information. Do not respond to this type of email and if you are in any doubt you should make your own contact with your bank for confirmation.

In order to minimise the amount of Spam received:

- Do not respond to Spam
- Do not try to unsubscribe from a Spam email - if you do, the spammer will know that your email address is valid and you will probably get more Spam emails
- Do not react to false virus reports. These reports tell you how to take measures against a so-called virus. In reality there is no virus, but following the instructions may damage your computer
- Delete any Spam emails that you receive

7.24 Disclaimer

The following disclaimer is appended to all email sent from the Council's email system to external recipients:

"This email and its attachments may be confidential and are intended solely for the use of the individual to whom it is addressed. Any views or opinions expressed are solely those of the author and do not necessarily represent those of Gateshead Council.

If you are not the intended recipient of this email and its attachments, you must take no action based upon them, nor must you copy or show them to anyone.

Communications by email are not guaranteed to be private or secure.

Please contact the sender if you believe you have received this email in error."

7.25 Council email addressing standard

Your Council email addresses is unique to you and is in the format of FirstnameLastname@gateshead.gov.uk
Where multiple employees share the same name, a numeric identifier will be added to the name field of the address to differentiate between them i.e.
FirstnameLastname1@gateshead.gov.uk
FirstnameLastname2@gateshead.gov.uk
FirstnameLastname3@gateshead.gov.uk

Where a departmental address is required it should be in the format of EnquiriesDepartment@gateshead.gov.uk

7.26 Monitoring of email

ICT Services make every effort to ensure the privacy of users' data, including email messages. Email content is not viewed during the course of normal systems administration, nor are files opened or read.

You should note that no absolute guarantee of privacy can be given. Operational requirements, such as action to investigate an undeliverable email message, may lead to systems administrators being exposed to the content of messages.

Any information obtained by ICT Services during the course of systems administration will be classed as confidential and will not be used or disclosed in the normal course of events. However, you should note that where routine systems management (i.e. technical management of the system to ensure that it is operating correctly) or administration indicates a breach of Council policy or the law, ICT Services will bring this information to the attention of the Council or other relevant authorities.

You should also be aware that authorised individuals within your Service may be granted access to emails during periods of absence, for business continuity reasons. Management are also able to access detailed reports of email usage by employees for both personal use and Council business use. Such reporting is not provided on a set basis but is available to managers in the normal course of an investigation, or on suspicion of inappropriate or excessive personal use of email by an employee.

8. *Information Sharing*

In some instances it is necessary for third party organisations outside the Council to have access to sensitive Council data, or to personal data for which the Council, under Data Protection legislation, is the responsible data controller. Such access might be at the Council's discretion or be a statutory or legal obligation. Examples might be (but are not limited to):

- where a commercial supplier is allowed remote or on site access for maintenance and support or development purposes to a computer system that processes personal or sensitive data (discretionary access),
- where Council data files might be stored off site by a commercial supplier (discretionary access),
- where data processed on Council computer systems is then transmitted onwards to a third party for further computer processing, (discretionary access)
- where a supplier needs a copy of the data from a computer system to produce printed or electronic output, such as bills, invoices, payment advices, emails etc.
- returns to central government (statutory access)

In discretionary cases a legally binding agreement must first be reached and documented with the third party organisation identifying the responsibility of the third party and its employees to keep the Council's data secure and not misuse the access they will have to the data. In statutory cases, Council employees should ensure that the method used to send or submit data to outside organisations provides an adequate level of security for the data. For further advice on this please contact the Councils Data Protection and Information Rights Officer in Legal and Corporate Services.

Where the outside organisation provides (for example) a secure web site (ie uses encryption) or similar facility specifically for the upload of the data to be shared, then this facility must be used by Council employees.

The use of internet based file sharing sites such as Dropbox and Skydrive are not permitted, as the processes and procedures that would enable automatic checking of documents to prevent personal and\or sensitive information being moved to these kinds of sites are not in place.

If it is necessary to send information of a personally identifiable or sensitive nature by email to an external recipient the data must be encrypted and where applicable, digitally signed. Users should note that password protection of a Word document or Excel spreadsheet or putting a CD or USB device in the post is not a secure method of safeguarding data and should not be used to transmit sensitive or confidential data. Please contact ICT Services for advice on encryption and digital signatures for this purpose.

Where the amount of information to be shared is too large for email, ICT Services can provide a secure file transfer service. This can be used as an alternative to secure email to transfer files containing sensitive or personal information that are too large to either send or receive by email between the Council and other organisations. The facility can be used from any computer with an internet connection to easily and securely upload and download files. Access is controlled by a username and

password. If this facility is more appropriate for secure information sharing, please contact ICT Services for advice on its use.

9. *Telecommunications*

9.1 Telephone systems

You must contact ICT Services before procuring any items of telephone equipment or software. ICT Services will ensure that only equipment meeting the Council's standards is procured, is installed and configured correctly and securely, and is compatible with existing systems.

If you have a requirement for new or additional telephone equipment or handsets you should contact the Corporate ICT Service Desk, or your Service based support if you have one, stating your requirements. ICT Services will in turn advise you of the available options and the costs associated with them. Whilst the procurement of all equipment is carried out by ICT Services, your own Service is responsible for funding it. Therefore you must ensure that you have obtained your line managers approval and also budgetary approval from your Service Budget Holder prior to placing the request to ICT Services to purchase equipment.

In order to ensure that telephone systems remain correctly configured and secure, access to system commands and special facilities are restricted to authorised employees only. If you have a requirement for advanced functionality or require changes to the default configuration of the telephone system you should contact the ICT Service Desk with details of the request.

Use of the Councils telephony and related systems may be monitored.

Each telephone extension can be set up with any one of a number of dialling access levels:

Internal and 999 calls only
Local calls
National and Mobile calls
International calls

By default, telephone extensions are configured with dialling restricted to internal and emergency calls only. If you require a change of access level to a telephone extension you must seek approval from your line manager, who in turn should contact the ICT Service Desk with details of the required change.

All outgoing calls from Council telephone systems are logged. The log records the date and time of the call, its duration, the originating extension and the number called. Monthly reports showing details of all calls made are provided to a nominated contact within each Service area and it is their responsibility to ensure that the reports are reviewed to identify potential signs of misuse.

When using a Council telephone you need to take care that the information being discussed is not overheard by passers-by. Additionally you need to be aware of the importance of checking the credentials of all callers requesting personal or otherwise sensitive information.

It is accepted that occasionally employees may need to make personal telephone calls whilst at work. However, you should make sure that the facility is not abused and office telephones are not unduly tied up with personal calls.

- Wherever possible personal calls should take place outside work hours, for example during lunch breaks.

- The amount of work time taken up by personal calls must be kept to a minimum.
- This applies to internal and external personal calls.
- It also applies to incoming as well as outgoing personal calls.

In the Civic Centre and where the facility exists at other Council offices all personal calls must be made using the 174 access code.

- A number of lines are dedicated at the switchboard for this purpose.
- Employees should wait for the availability of a 174 line to make a call.
- The number of lines is limited so it is in everyone's interest to keep calls short and to a minimum.
- The 9 access code should not be used for personal calls.

The use of the 174 prefix allows all personal calls to be identified. A monthly report lists all personal calls made at each extension showing:

- The time of the call.
- The duration of the call.
- The number called.
- The cost of the call.

The report is used to charge individual employees for personal calls.

- Income will be collected as soon as possible after the report becomes available.
- Employees must pay promptly.
- Arrears can not be carried over to the following month.

Where establishments do not have a switchboard, or the switchboard does not have a logging facility, arrangements should be made to record personal calls manually by using, for example, personal record sheets or an honesty book to record the number, location and duration of calls.

9.2 Fax machines

Confidential information can be vulnerable when sent by fax to others. Mail is usually sealed, but faxed documents can be read by anyone who has access to the fax machine. For this reason careful consideration should be given to the positioning of fax machines.

You should be aware that the responsibility for the fax lies with the person sending, or asking for the fax to be sent. You should make sure consideration is given to whether faxing is the most appropriate option in light of who the fax is being sent to, who has access to the fax machine, the sensitivity and confidentiality of the information and the consequences of the information being read by someone other than the person it is addressed to. Care should also be taken to ensure that you send a fax to the correct number to minimise the risk of unauthorised viewing.

The 'ring ahead and confirm system' should be used especially when faxing confidential or sensitive data. The intended recipient should be called to confirm that a fax will be sent to them and then they should be called to check that it was received.

Personal use of fax machines must be paid to your admin section at the time of sending the fax.

9.3 Voice mail

In its basic format a voice mail system can be considered as a replacement for a traditional telephone answering machine. When used correctly voice mail systems offer a convenient method for callers to leave non-urgent messages when there is no one available to answer the telephone. It is important therefore that you adhere to the following points in order to ensure that system is used effectively:

- Check for messages regularly and act upon them at least twice a day
- Delete messages once you have listened to and acted upon them
- Leave details on your greeting message of an alternate extension number so that the caller has the option to speak to a colleague on urgent matters
- If you will not be accessing your voice mail during the working day, change your greeting to inform callers when their message will be acted upon
- Keep your greeting message clear, concise and professional
- Ensure that you keep your PIN code confidential, do not disclose it to anyone and ensure that you change it regularly
- Do not use simple number sequences for your PIN code, such as 0000, 1111, 1234 etc

All shared or group voice mailboxes must have an owner identified when the mailbox is requested. Sections of this policy relating to personal mailboxes should be adhered to when managing shared voice mailboxes. Additional rules should also be in place relating to when to delete a message from the mailbox and how to identify a message as having been dealt with. It is the responsibility of the mailbox owner to ensure that there are specific rules relating to the management of shared mailboxes, and it is the responsibility of all employees with access to shared mailboxes to abide by those rules.

You should be aware that authorised individuals within your Service may be granted access to your voice mailbox during periods of absence, for business continuity reasons. If you are off work unexpectedly it is advisable that you call your voice mailbox and change your greeting to inform callers that you are unable to take telephone calls and advise them of an alternative number to call.

9.4 Mobile phones

The handset and all equipment remains the property of the Council and must be returned if you leave the employment of the Council

If you are issued with a mobile phone, the handset and all equipment will remain in your possession until you are asked to return it.

A register of use will be kept if you are issued with a pool mobile phone and you should sign the phone ‘out and in’ on the same working day.

All pooled mobile phones should be returned to the relevant section at the end of each working day or shift or as soon as possible afterwards. Phones should be stored in a locked, secure place in the relevant section when not issued.

You must make sure that the mobile phone is kept in a secure place. You must take particular care to keep it safe when you are carrying it. You are personally responsible for the security and day to day maintenance of the phone.

You must not allow use by unauthorised persons.

Please report any faults or difficulties to ICT Services as soon as possible.

If you lose the handset or any equipment please report it to your ICT Services immediately.

Private use of the handset is allowed but should be limited to essential calls. You will be required to pay for any private calls shown on the regular itemised bill. Private use will be monitored and any misuse will result in it being withdrawn.

All access to the Internet, television, video, radio and other media, whether for Council business purposes or personal use, must be via a method approved in advance by ICT Services.

SIM cards must not be removed from any Council owned device. It is not permitted to use a council SIM card in a non-council device (including mobile phones, smartphones, tablet computers).

9.5 Mobile radios

When using a Council mobile radio system you need to be aware that the information being discussed may be overheard by passers-by, both near to you and in the vicinity of other users of the radio system.

You should make sure consideration is given to whether radio communication is the most appropriate method, in light of who else is using the radio system, the sensitivity and confidentiality of the information under discussion and the consequences of the information being heard by someone other than the person it is intended for.

The handset and all equipment remains the property of the Council.

If you are issued with a mobile radio, the handset and all equipment will remain in your possession until you are asked to return it.

A register of use will be kept if you are issued with a pool mobile radio and you should sign the radio ‘out and in’ on the same working day.

All pooled mobile radios should be returned to the relevant section at the end of each working day or shift or as soon as possible afterwards. Radios should be stored in a locked, secure place in the relevant section when not issued.

You must make sure that the mobile radio is kept in a secure place. You must take particular care to keep it safe when you are carrying it. You are personally responsible for the security and day to day maintenance of the radio.

You must not allow use by unauthorised persons.

Please report any faults or difficulties to your Administrative Section as soon as possible.

If you lose the handset or any equipment please report it to your Administrative Section immediately.

10. *Wireless Technology*

Developments in the field of wireless connectivity have changed the technology beyond all recognition in recent years and further innovation continues to appear regularly. Due to the rapidly changing nature of the technology it is difficult to specify in detail within this policy what is and what is not appropriate, therefore the following statement applies:

Under no circumstances should any attempt be made to install or connect any device not supplied by the Council to its network using wireless technology without prior consultation with ICT Services. Any such use or connection must be in compliance with the Council standards set out at that time.

For the purposes of this policy, the term wireless is defined as being any technology that does **not** use a wired connection such as Wi-Fi, Bluetooth, Infrared, Wi-max, Microwave, 3G, 4G, GPRS etc.

11. *Reprographic Equipment*

11.1 Cameras

Only cameras procured through ICT Services may be connected to the Council network or computers. Personally owned cameras must not be connected to prevent a number of potential problems occurring which may expose the Council to risks such as:

- Conflicts between versions of home and corporate software occurring when the camera is connected to Council equipment
- Non-compliance with software licensing agreements - it may be a breach of the licence agreement to install the necessary software or drivers for the camera onto both a home and a Council computer, or to use the software for anything other than domestic use
- Uncertainty of ownership of data – e.g. a personal camera used to take pictures for work purposes would create uncertainty over the legal owner of the images, additionally family and friends may then have access to those images
- Insurance claims for loss or damage – e.g. if a personal camera being used to take pictures for work purposes is dropped and damaged it may not be covered by either Council or home insurance

All camera usage must be in accordance with the relevant legislation.

11.2 Printers

Confidential information can be vulnerable when sent to a printer. Printed documents can be read by anyone who happens to be passing by the printer, therefore you should ensure that you collect printouts without undue delay.
If you are using a multifunction device (MFD), remember to always log out when you have finished.

Care should also be taken to ensure that you send a print to the correct printer to minimise the risk of unauthorised viewing.

11.3 Photocopiers & Scanners

As with printers care should be taken not to leave sensitive or confidential information on a photocopier or scanner.

Consideration should also be given to the document you are copying to ensure you are not in breach of copyright legislation.

11.4 Use of Recording Equipment

Recording equipment includes any device that records a person's image or voice. All use must be in accordance with the Police and Criminal Evidence Act.

11.5 Video Conferencing

When using a Council video conferencing system you need to be aware that the information being discussed may be overheard by passers-by, both near to you and in the vicinity of other users of the conferencing system. To reduce this risk you should ensure that camera and microphone equipment is located in rooms where there is little possibility of being accidentally seen or overheard.

The auto-answer function must be disabled so that any incoming conferencing calls are manually accepted rather than being automatically initiated.

You should ask everyone who is participating in the video conference to introduce themselves at the start of the meeting.

If a conference is to be recorded all participants should be made aware of this at the start and consent must be sought before proceeding.

You should make sure consideration is given to whether video conferencing is the most appropriate method of communication, in light of who else is using the system, the sensitivity and confidentiality of the information under discussion and the consequences of the information being heard by someone other than the person it is intended for.

11.6 CCTV

All CCTV equipment must be used in accordance with the relevant legislation and in line with the guidelines published on the Information Commissioners website.

12. *Home / Remote Working*

All work from home must be carried out in accordance with the Councils Home Working Policy. In addition to this when using Council systems or equipment or using any equipment to work on Council business away from Council premises, the ICT Security Policy generally and the following rules specifically will apply:

- All information related to the business of the Council must be password protected
- All work, in particular that where personally identifiable or sensitive information is involved, should be carried out in a position where it cannot be seen by others
- All reasonable precautions should be taken to safeguard the security of all Council equipment or information regardless of the medium it is stored in – paper, disk, CD, DVD, USB device, laptop etc
- In accordance with principle seven of the Data Protection Act 1998, appropriate measures must be taken to ensure the security of personal data that comes into your possession in the course of your employment to prevent it from theft, loss, destruction or harm either accidental or malicious
- All work related files saved on a portable storage device or laptop should be transferred to a Council server as soon as is practical, and deleted from the storage device.

13. *Payment card security*

The Council is required to take particular care over the security of the details of payment cards (debit, credit and pre-payment cards) that customers use to make payments to the Council. So, the Council has a policy on how card transactions must be processed. The policy must be adhered to by all employees involved in processing card transactions or in the support of systems used to do this. Full details of this policy can be found in the Council's Payment Card Industry (PCI) Data Security Standard Policy and Procedures.

14. *Information Classification*

Information should be classified according to the following Government classification scheme to ensure that all persons know what level of security should be applied.

Personally Identifiable - Information that can be used to identify living individuals. These documents are likely to be bound by the requirements of the Data Protection Act.

Organisationally Sensitive – This classification includes any information relating to activity that does not identify living individuals but may cause operational difficulties if the information became corrupted, compromised, unavailable or disclosed.

Public Information – Information that does not identify individuals or include organisationally sensitive information and has not been published. This information may be subject to access requests under the Freedom of Information Act.

Published information – Information that has been published, including classes of information identified in the Council's Freedom of Information Act publication scheme.

Each Service must take responsibility for their file and folder permissions in line with the Councils Records Management Policy. Please contact ICT Services for advice on how this should be done.

15. *Incident Reporting*

Incident reporting and monitoring provides a method of notifying any unwanted events (such as virus infection, deliberate intrusion, attempted information theft, loss or theft of equipment) so that they can be detected, acted upon, analysed and measures put in place to reduce the risk of it happening again.

If you know of a security incident or suspect someone is misusing the Council's computers either deliberately or accidentally you must report it to your line manager or email incidentreporting@gateshead.gov.uk as quickly as possible.

Your Information Asset Owner in turn is responsible for ensuring that the incident is recorded and that the Council's Incident Reporting Group is informed without undue delay.
The procedure for incident reporting is covered in more detail in the Council's Confidential Reporting Code, which is available on the Intranet.

16. *Monitoring of Activity*

The Council reserves the right, consistent with the relevant legislation, to exercise control over computer resources and to monitor their use to ensure efficient operation, to detect misuse and to supply evidence, if required, for use in disciplinary or legal proceedings.

16.1 Privacy and Confidentiality

ICT Services makes every effort to ensure the privacy of your data, including email messages, Internet browsing logs and files held on computer systems. Email content and web browsing logs are not viewed during the course of normal systems administration, nor are user files opened or read.

You should note that no absolute guarantee of privacy can be given. Operational requirements, such as action to investigate an undeliverable email message or to recover a corrupted file, may lead to systems administrators being exposed to the content of messages or files.

Any information obtained by ICT Services during the course of systems administration will be classed as confidential. You should be aware that where routine technical management of a system indicates a breach of the Council's security policies or the law, ICT Services will bring this information to the attention of the Council or other relevant authorities.

You should also be aware that authorised individuals within your Service may be granted access to emails and files stored on computers during periods of absence, for business continuity reasons. Content of emails, web-browsing logs and files stored on computers may also be examined during the course of properly authorised investigations into breaches of Council rules or the law.

By using Council systems you accept that all use may be monitored.

16.2 Internal Audit

Audit of adherence to the Policy and its supporting procedures and standards will be carried out by the Council's Internal Audit Service as part of its routine planned audit work as authorised by the Council's constitution and appropriate legislation.

Breaches of the Policy and its supporting procedures and standards will be investigated as considered appropriate by Internal Audit.

17. *Misuse*

Any breach of the Policy will be viewed seriously and may result in action being taken under the Council's Disciplinary Procedures, Police investigation and / or legal action, as the Council deems appropriate. In some instances failure to adhere to the policy may also result in legal action being taken against employees by third parties outside the Council. The legislation that applies to Computer use/misuse within the Council is outlined below in section 18.

18. *Relevant Legislation and other Council Policies*

The following legislation and Council policies should be read in conjunction with the policy:

- Data Protection Act 1998
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Human Rights Act 1998
- Lawful Business Practice Regulations 2000
- Freedom of Information Act 2000
- Obscene Publications Acts, 1959 and 1964
- Trade Marks Act 1994
- Public Interest Disclosure Act 1998
- Regulations of Investigatory Powers Act 2000
- Police and Criminal Evidence Act 1984
- Council's Fraud and Corruption Policy
- Council's Confidential Reporting Code
- Council's Code of Conduct
- Council's Records Management Policy
- Council's Home Working Policy
- Council's PCI Data Security Standard Policy and Procedures
- Council's Mobile Device Usage Policy - stored in Hints & Tips on iPads
- Social Media Policy – currently under development

19. *Policy Review*

The policy will be reviewed by the Information Security Group at least annually and whenever changes in technology, legislation and risk occur. Any amendments or updates to the policy will be communicated to employees as appropriate.

20. *Glossary*

3G – Third Generation technology used primarily by mobile phones to allow the simultaneous high-speed transfer of voice and data

Bluetooth – a technology used to connect devices using wireless over a short distance

CCTV – Closed Circuit Television

CD – Compact Disc

Chat Room – an online site in which allows people to communicate by broadcasting messages to others on the same site in real time

Dropbox - an example of an internet based file sharing site that allows you store files to an external storage area and access them from multiple locations/devices. Skydrive is another example.

DVD – Digital Versatile Disc

GPRS – General Packet Radio Service. A mobile technology allowing transfer of data

ICT – Information and Communication Technology

Infrared – a technology that utilises infrared light for the exchange of data between devices

Instant Messaging – a form of real-time communication between two or more people based on typed text

ISO – International Standards Organisation

Peer-to-Peer – a commonly used protocol for downloading software, MP3 music or other files with other ordinary users on the Internet

Spam – unsolicited or undesired bulk email advertisement messages

USB – Universal Serial Bus. A “plug and play” method of connecting peripheral devices to a computer without the need to install expansion cards.

Wi-Fi – a term used to describe the underlying technology of wireless local area networking

Wi-max – Worldwide Interoperability for Microwave Access. A standards based wireless technology that provides high-throughput broadband connections over long distances.