ICT Acceptable Use Policy

1. Introduction

1.1. The Council is dependent on Information Communication Technology (ICT) to deliver its services. The proper, secure and appropriate use of ICT is vital to maintaining and further developing good customer service.

1.2. This policy describes the acceptable use of ICT that will protect the interests of our customers, ICT users and the Council, so that

- The use of ICT complies with legal requirements;
- The maximum benefit is obtained from our investment in ICT facilities;
- Risks arising from improper use of information, identity or equipment are minimised; and
- Individual users have confidence that they can only be held accountable for their own actions (and not those of others).

1.3. The following sections clearly describe what is identified as acceptable use and what is not. Deliberate misuse of ICT facilities is likely to result in disciplinary action.

1.4. In this policy, excessive use is considered to be use that interferes with an individual's performance at work, or the work of others, or results in noticeable costs for the Council. Incidental use is that which occurs for short periods, probably at lunchtimes or before or after work.

1.5. Managers in doubt about particular situations should seek advice from the HR Department.

1.6. Some departments may use 3rd party applications in order to carry out their day to day work. You may have to use specific applications for tasks within your role. Access to some of these applications is controlled by the use of usernames and passwords. The protocols described below apply to the use and management of these applications.

2. Scope

2.1. The policy covers everyone who uses Council's ICT facilities. Specifically, Council's employees on permanent, temporary and fixed term contracts, temporary or casual staff, volunteers, contractors and other staff employed by a third party and who use Council's facilities.

2.2. The “Council’s ICT facilities” means all ICT equipment and the information stored on it that is owned by Council’s or for the use of which Council’s can be held responsible. This includes all digitally stored and transmitted information, Personal Computers (PCs), portable devices (such as laptops, Personal Digital Assistants (PDAs), smart phones, mobile phones, tablet devices and digital pens), all storage devices(e.g. CDs, memory sticks, external hard drives) and all Council’s telephony services.

3. Sources of Help

3.1. The ICT Service desk provides a single point of contact for all staff with any operational problem or service request.

4. Access to Systems

4.1. Access to Council’s ICT systems is controlled by usernames and passwords. You must not share your password with anyone else. Keeping passwords secret helps to protect you from identity theft at work. You will be held accountable for actions carried out under your username and password.

4.2. The Council reserves the right to log and monitor your access to the Council systems. This is an express term in your terms and conditions of employment and the Council's right to use monitoring is covered in your contract of employment

4.3. When you receive a password from ICT Services staff you must immediately change it to one that only you know. For help on choosing secure and memorable passwords speak to the ICT Service desk.

4.4. Passwords must meet complexity requirements. These requirements can be obtained from the ICT Service desk.

4.5. You must not disclose your password/s to anyone

4.6. If you are provided with remote access to Council’s systems you may be given a remote access token such as a Cryptocard, RSA token or an SMS message. The token must be kept safe and not stored with the device used for remote access.

4.7. If you need access to a specific application to carry out your role, you will be informed on the process and protocols applicable to that specific piece of software.

4.8. Policies governing accessing the Council’s network and data from other locations will be covered by the Remote Working Policy.

5. Access to Data and Personal Information

5.1. Access to data and information is provided to you to deliver and improve Council service delivery. You may only access information on Council’s systems if you have been properly authorised to do so and need the information to carry out your work. In this way the Council complies with its legal obligations and you are not at risk of acting illegally.

5.2. As part of your job, you might have access to data that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. You are trusted to act responsibly with this data, and it must only be used to help you to carry out your job. It must not be passed directly or indirectly through neglect, to people who have no right to see it.

5.3. Unauthorised release of this personal information is likely to be treated as misconduct under our disciplinary procedures. You could also be held legally liable for actions that break the Data Protection Act, such as failing to ensure the confidentiality of data.

5.4. Further information on the Act is available on the Council's web pages.

5.5. It should also be noted that unauthorised access to, or modification of, data is a criminal office under the Computers' Misuse Act 1990.

5.6. In accordance with the Freedom of Information Act all information held by the Council should be made available on request unless covered by exemptions in the Freedom of information Act or Data Protection Act for example, personal data.

6. Use of the Council's Internet Connection

6.1. Access to the internet is provided to you to improve Council service delivery. The connection to the Internet is corporately owned, and therefore you should understand that there is no automatic right to any privacy relating to activities conducted through the Council's internet connection.

6.2. Incidental personal use of the internet is permissible provided that it is limited to a reasonable amount, is not misused (see below) and does not interfere with work responsibilities.

6.3. The Council reserves the right to monitor internet use. This is an express term in your terms and conditions of employment and the Council's right to use monitoring is covered in your contract of employment.

6.4. You must not use the Council's internet connection in any way that might bring the Council into disrepute. Any access to the internet from the Council's network can be traced back to the Council. This includes access to:

- Your private e-mail if accessed via the corporate network;
- Comments made on any Blog, discussion group, wiki or other social networking site; and
- Any other form of access to resources made available through the internet.

6.5. If, as part of your incidental personal use of the internet, you need to provide an e-mail address when you order goods and services you must provide a private e-mail address, NOT your Council e-mail address.

6.6. If your Line Manager is concerned that you are making excessive private use of internet access or accessing inappropriate sites they shall consult the HR Department and take appropriate action.

6.7. If you access information accidentally which is of an offensive, discriminatory or criminal nature, you should immediately report this to your Line Manager.

6.8. Misuse of Internet access includes but is not limited to:

- Access to sites that contain pornographic, exploitative, offensive, discriminatory or criminal content;
- Excessive time spent on the internet for non-work related reasons; and
- Excessive use that overloads the corporate internet connection, such as streaming media or downloading video for private use.

6.9. Access to internet sites, which contain pornographic, exploitative, offensive, discriminatory or criminal content, will result in disciplinary action. If the access is illegal, the Police will be informed.

7. Use of E-Mail

7.1. Unless by specific agreement with your Line Manager, you may not use any e-mail address other than one specifically allocated to you.

7.2. E-mail is provided to you in order to improve Council service delivery. This system is a corporately owned asset and, therefore, you should understand that there is no automatic right to the privacy of email or messages.

7.3. The Council reserves the right to monitor and archive emails. This is an express term in your terms and conditions of employment and the Council's right to use monitoring is covered in your contract of employment.

7.4. You may use the e-mail system for incidental personal use, for example for social correspondence with Council's colleagues, provided that it is limited to a reasonable amount. Such use must not include any of the categories listed below under misuse of e-mail and must not interfere with work responsibilities.

7.5. Council's may filter email content, and block any email that is deemed inappropriate or potentially harmful to the council network

7.6. If you are unexpectedly absent from work for a period of time, your Line Manager may arrange for someone else to access your mailbox and deal with outstanding matters. Messages to your email account may be diverted and copied to other accounts so that they can be dealt with in your absence.

7.7. If you are planning to be absent, you should make appropriate arrangements for your mail to be diverted if necessary and set an out-of-office message to inform those emailing you of your return date.

7.8. If your Line Manager is concerned that you are making excessive private use of the system they should notify the HR Department. .

7.9. If you are sent an email, which contains material that you feel is offensive, discriminatory, or criminal you should immediately report this to your line manager.

7.10. Misuse of the email and messaging system includes, but is not limited to:

- Sending pornographic, exploitative, offensive, discriminatory or inappropriate content;
- Excessive personal use of the email system for non work-related reasons;
- Using your Council's e-mail address when negotiating or confirming private contractual arrangements such as ordering goods and services. You should use a private e-mail address for private orders placed via the Council's Internet connection;
- Forwarding chain emails that ask you to forward them to many others;
- Sending emails from another user's e-mail address;
- Sending or receiving copyright protected or other licensed material without the appropriate permissions.

7.11. Writing or forwarding emails or messages that contain pornographic, exploitative, offensive, discriminatory or criminal content will result in disciplinary action. If the content is illegal, the Police will be informed.

7.12. Only use Council provided email addresses to send Council related information to external email addresses.

7.13. If you have to send personally identifiable or sensitive data to external email addresses, the data should be encrypted to a minimum standard. This minimum will be 128-bit AES. Sensitive and person identifiable information and data must not be emailed unencrypted.

7.14. Any users issued with a GCSx email address will be subject to additional rules and regulations that govern the use of those facilities

8. Operational Data and Information

8.1. Data and Information that is used to deliver services should be held on corporate systems in line with ICT Services strategic directions. The ICT Technical Officer can advise on an appropriate solution.

8.2. All data should be saved to the shared network drives and not on the hard disc (C: drive) of your PC. Data on the network drives is backed up nightly by ICT Services and can be retrieved in the event of a failure. Any data not stored on the network drives will not be backed up and will not be retrievable. If you do not have access to the shared drives you should seek advice from the Service Desk on how to back up the data.

8.3. Any data saved on portable devices should be saved to the Council's network drives as soon as is practically possible.

8.4. Data and information should only be kept for as long as is needed for legal, operational, or other business reasons. Information should be retained in accordance with the Council's Retention schedule. Advice in any specific instance can be obtained from the Data Protection Officer.

8.5. The downloading of copyright protected content without the licensor's permission is illegal and the license conditions must always be adhered to. This can also apply to other copyright material such as music and video files. The person carrying out copying without a license or permission to do so is legally liable and may be prosecuted.

9. Use of Software

9.1. Software is provided to you to deliver and improve Council services.

9.2. Only software properly purchased and approved by ICT Services may be used on Council computer systems. You may not install software acquired through other means on to any Council's owned ICT assets, including desktop computers, laptops, smart phones, tablets etc

9.3. You may not use any software service delivered via the internet (e.g. Google Docs or other 'cloud' services) for any work related activity unless approved or enabled through ICT Services. ICT Services will investigate the appropriateness of the software and provide information to Line Managers so that a data risk assessment can be carried out.

9.4. The use or copying of software without the licensor's permission is illegal and the terms and conditions of software licenses must always be adhered to. Any person carrying out illegal software copying is legally liable and may be prosecuted.

9.5. Changes may not be made to the configuration of software except by ICT Services staff or someone authorised by them to make the changes.

9.6. Whilst it is your responsibility not to deliberately change the configuration of your computer software, it is possible for software to be installed on a machine without the full knowledge of the user. If you discover software that has been installed in an unsolicited manner, contact the ICT Service Desk.

9.7. If your needs cannot be met by the software solutions provided to you please discuss the matter first with your line manager and then the ICT Service Desk.

10. Use of ICT Hardware

10.1. All ICT hardware is provided to you to deliver and improve Council services. The Council is responsible and liable for the hardware. You are expected to take reasonable care of the hardware.

10.2. All hardware, including significant peripheral devices (such as screens and printers) is recorded on the ICT Services inventory and must not be moved from its location without notification to the ICT Service Desk who can then record the change in location. If you move equipment yourself, neither you nor the equipment is covered by insurance.

10.3. If you are away from your computer for a short period you should lock access (e.g. by using the Ctrl-Alt-Del keys and select "lock computer"). If you are away for longer periods then switch off the machine, this minimises any security risk and reduces overall power consumption.

11. Equipment Connected to the Network

11.1. No equipment of any sort may be connected to the corporate network without agreement and approval by ICT Services; the ICT Service Desk must be contacted before any connections are made. Other network solutions are available for third parties, contractors and visitors.

11.2. You may not reconfigure your network connection in any way.

11.3. You are not permitted to enable or install any facility that allows remote control of the computer. The ICT Services support team will install any such software to assist their support activities if it is needed.

12. Wireless Networks

12.1. Wireless networks may be provided as part of the Council's infrastructure. They allow for flexible working but can introduce additional security vulnerabilities unless used and configured correctly.

12.2. Never attempt to change the way the wireless connection is configured. It will be set up to encrypt the data that passes between your machine and the wireless access point to prevent anyone else listening in or using the connection without permission.

12.3. Please refer to the Remote Working Policy for clarification on the use of wireless networks when working away from the Councils offices.

13. Portable Devices

13.1. You may be provided with portable devices such as laptops, tablets, PDAs or smart phones in order for you to work in a variety of locations. You must be careful to prevent the equipment being lost or stolen.

13.2. All portable devices will be encrypted by ICT Services before they are issued to staff. This is to ensure that if the device is lost or stolen that data cannot be accessed by unauthorised personnel.

13.3. When travelling on the mainland, do not leave a laptop or other device in your car. A device left in an unattended car is not covered by insurance.

13.4. If you use a portable device (such as a laptop or a Smartphone) on the train or other public area, never leave it unattended. Also be aware that information that you are reading might be visible to other people.

13.5. Mobile devices are provided for you to use in order to do your job, no one else, including family members, should use them.

13.6. The acceptable use policy for internet and e-mail use applies to mobile devices when outside of the council network.

13.7. Devices used to transfer data (e.g. memory/usb sticks etc) should be encrypted. Only devices approved by ICT services will be allowed.

14. Disposal

14.1. When you leave your job you must arrange the return of all portable devices to the ICT Services Department. They must not be redeployed locally without permission from ICT Services.

14.2. When hardware is replaced or is no longer required, the original hardware will be returned to ICT Services staff and redeployed to other staff if possible. If it is to be disposed of, the disposal will be according to industry standards.

15. Use of Voice Services

15.1. Voice services and equipment are provided to you in order to promote flexible working and improve Council service delivery.

15.2. Incidental telephone use for private calls without charge is permitted, provided that it is limited to a reasonable amount. Such use must not interfere with work responsibilities.

15.3. If your Line Manager is concerned that you are making excessive private use of the telephone system they can take action.

15.4. You are expected to follow the corporate standards for telephone use:

- Calls should be answered promptly
- Calls should not be screened by using the voicemail facilities or answer-phones
- You should give your name and team when answering the telephone.
- You should follow local procedures for giving out telephone numbers to the public
- Internet or email access via a mobile telephone or Blackberry is subject to this acceptable use policy.

15.5. You must adhere to the operating instructions for mobile devices such as phones at all times.

15.6. You are responsible for the safekeeping of mobile phones and accessories and instructions provided with it.

15.7. If a mobile phone goes missing, it must be reported immediately to enable the line to be blocked from further use.

15.8. Do not make or answer calls whilst driving. For guidance on the use of mobile phones in cars see the Council's intranet Health and Safety pages.

- Do not allow anyone else to use your mobile phone.
- Mobile phones and all accessories must be handed back when you leave your job.

16. Review

This Policy shall be reviewed annually by staff of the ICT Department and submitted for approval to the relevant committee.

Law relating to this document:
Leading Statutory authority: Data Protection Act 1998
Human Rights Act 1998
Regulation of Investigatory Powers Act 2000
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)
Employment Practices Data Protection Code (on the Information Commissioner's website)
D Marcus, Feb 2013, ICT Technical Officer