Finance and Resources Committee

10.00am, Thursday, 23 May 2019

Information and Communications Technology Acceptable Use Policy 2019

Item number	7.21
Executive/routine	
Wards	
Council Commitments	

1. Recommendations

1.1 To approve the updated Information and Communications Technology Acceptable Use Policy 2019.

Stephen S. Moir

Executive Director of Resources

Contact: Nicola Harvey, Head of Customer and Digital Services,

Customer and Digital Services, Resources Directorate

E-mail: Nicola.harvey@edinburgh.gov.uk | Tel: 0131 123 4567

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Information and Communications Technology Acceptable Use Policy 2019

2. Executive Summary

2.1 The Policy Statement on Information and Communications Technology Acceptable Use Policy 2019 is being updated to meet the requirement under the Information Security Policy to publish a statement on the Acceptable Use Policy.

2.2 The updated Acceptable Use Policy has been written in line with best practice guidelines encapsulated in the Scottish Government's Cyber Security Resilience Framework and the Cyber Resilience strategy for Scotland.

3. Background

3.1 The ICT Acceptable Use Policy was last revised in December 2014. As part of our commitment we have updated the ICT Acceptable Use Policy 2019 to align with current best practice, legislation and to better defend against emerging and increased cyber-security threats to our operations. This update to the policy will also enable the Council to implement and support the closure of some Internal Audit findings.

4. Main report

4.1 The information contained in the ICT Acceptable Use Policy 2019 is based on guidance as at January 2019. The ICT Acceptable Use Policy has been written in line with guidance from the Council's Cyber Security specialists, the Information Governance Uni Cyber, including the statutory Data Protection Officer, CGI's Security Team, Scottish Government and that published by other public agencies and authorities such as the National Cyber Security Centre.

4.2 This policy applies to all 'individuals' (Councillors, employees, contractors, agency workers, volunteers and agents) who use our information and ICT equipment.

5. Next Steps

5.1 The updated Policy on ICT Acceptable Use will be published on the council web-site in June 2019.

5.2 The existence of the updated policy and the requirements it places on those who use the Council's ICT systems will be communicated and embedded through local induction arrangements and by building this into our Cyber Security Awareness and Training Programme and associated contractual provisions for external suppliers.

6. Financial impact

6.1 A breach of cyber security and, or subsequent breach of the General Data Protection Regulations (GDPR) due to not achieving the standards and best practices of the Scottish Government's Public Sector Cyber Security Action Plan and other best practice frameworks could lead to significant financial penalties.

7. Stakeholder/Community Impact

7.1 The ICT Acceptable Use Policy 2019 outlines our commitment to support the users of technology and deliver a Council that works for all its citizens.

8. Appendices

8.1 Appendix 1 – Policy Statement.

Appendix 1

Policy Statement: Acceptable Use of Information and Communications Technology

May 2019

It is the aspiration of the Council to create a culture which recognises the importance in the safe use of information and communications technology (ICT) for work purposes. This acceptable use policy has been written not only to protect Council electronic assets, data and information but to ensure that best practice is followed.

Author

Customer and Digital Services, with contributions from members from the Council's Cyber and Information Security Steering Group.

Scope

This policy applies to all Council employees, Councillors, Contractors, agency workers, volunteers and agents who use our information and ICT Equipment.

Purpose

The purpose of this policy is to provide a clear framework to be applied by the Council which governs the use of its network, website, digital services and data security.

Review

The policy will be reviewed as and when a change to the existing policy deems this necessary, primarily because of: changes to legislation, best practice and guidance from specialist bodies such as the National Cyber Security Centre (NCSC).

ICT Acceptable Use Policy 2019

1. General Applicability
2. System Access
3. Internet email and social media use
4. Clear desk, clear screen and secure print
5. Working remotely
6. Software use
7. Telephony (Voice) equipment use
8. Actions upon termination of office / employment / engagement
9. Reporting
10. Appendix 1 – Legal provisions

1. GENERAL APPLICABILITY

This policy covers the security and use of all Council information and Information and Communications Technology (ICT) equipment. It also includes the use of: e-mail, the internet, voice, and mobile IT or associated systems (e.g. printers, phones etc.).

Technology is increasingly used to process and share information both internal and external to the Council and must be undertaken in a manner that fully protects the rights of individuals and the reputation of the Council. It is also governed by legislation that is often updated following events or as technology evolves.

Individuals are required to review and fully adhere to this policy but should always take advice as described throughout this document.

This policy applies to:

- all 'individuals' (Council employees, Councillors***** contractors, agency workers, volunteers and agents who use our information and IT equipment);
- all information, in whatever form, relating to our business activities worldwide;
- all information handled by us relating to other people and organisations with whom we deal. It also covers all IT and information communications facilities operated by us or on our behalf.

*******Councillors must also abide by the specific and supplementary requirements relating to ICT in the Councillors' Code of Conduct.*

Misuse of computer equipment

This is a serious offence governed by law (Computer misuse act 1990). Failure to follow this acceptable use policy may result in:

- disciplinary action including immediate dismissal; and
- a report being made to the Police or
- other legal action being taken.

All data that is created and stored on our computers or systems, operated on our behalf, is the property of the Council and there is no official provision for individual data privacy. However, wherever possible, we will avoid opening personal emails.

IT system activity will be logged where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of Council policy or where a law has been broken.

Monitoring and Controls

The Council have the right (under certain conditions) to monitor activity on our systems, including the use of internet, email, and other forms of electronic communication, to ensure system security and effective operation, and to protect

against misuse. Any monitoring will be carried out in accordance with audited, controlled internal processes and in-force legislation.

Relevant legislation that applies to the use of Council computer systems is shown in Appendix 1.

Changes in Guidance

Best practice around both cyber and information security continues to evolve. The Council also looks to introduce both new technologies and make changes to existing ones to improve its operation. Therefore, individuals who use our systems should pay attention to the latest guidance around best practice that will be provided on our intranet or by email.

For additional information or clarification see the ICT Security Web Pages on our intranet or contact Cyber Security within Digital Services at ict.security@edinburgh.gov.uk

2. SYSTEM ACCESS

Access to our systems is controlled using user identification numbers (user IDs), PIN numbers, passwords and/or tokens.

All user IDs and passwords are uniquely assigned to named individuals. Consequently, each named individual is accountable for their actions on our IT systems.

Individuals must not:

1. Allow anyone else to use their user ID, token, or password on any Council IT system.
2. Leave their user accounts logged in at an unattended and unlocked computer.
3. Use someone else's user ID and password to access the Council's IT systems.
4. Leave their password unprotected, for example write it down thereby making visible to others.
5. Make unauthorised changes to our IT systems or information.
6. Attempt to access data that they're not authorised to use or access.
7. Exceed the limits of their authority or their specific business need to use the system or data.
8. Connect any non-Council authorised device to our network or IT systems.
9. Store Council data on any non-authorised Council equipment.
10. Give or transfer our data or software to any person or organisation outside the Council without our authority.
11. Use computer equipment as a means of breaching our policies or to break the law.
12. Look to subvert any IT or other security measures in place.

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority regarding use of IT systems and data.

3. INTERNET, E-MAIL AND SOCIAL MEDIA USE

Council internet, email, and electronic communication is intended for business use. Reasonable personal use is permitted where:

- it doesn't affect the individual's business performance;
- the use is not detrimental to the Council in any way;
- the use is not in breach of any term and condition of employment; and,
- the use does not place the individual or the Council in breach of statutory or other legal obligations.

All individuals are personally accountable for their actions on the internet and email systems.

Individuals must not:

1. Use the internet, e-mail or social media with the purpose of harassing, bullying, abusing, intimidating or victimising individuals or groups.

2. Use the internet, e-mail or social media to breach the Public Sector Equality Duty or the Council's policies in respect of Equality, Diversity and Rights.

3. Use profanity, obscenities or derogatory remarks in any communications using the internet, e-mail or social media.

4. Download, send, forward or fail to delete any data which the Council considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.

5. Use the internet to research, access or disseminate extremist material in contravention of any UK Counter Terrorism legislation.

6. Use the internet, email or social media to:
    a. make personal gains or conduct a personal business,
    b. gamble,
    c. breach any other Council policy or
    d. break the law.

7. Use the internet, email or social media without approval from their line manager or the Council's Cyber Security Team to:

    a. Place any information on the internet that relates to the Council or, expresses any opinion about the Council.
    b. Send personal, sensitive or confidential information externally about any 3rd party without ensuring appropriate encryption is in place.
    c. Forward Council email or upload data to a personal (non-Council) email account (for example a personal Hotmail account).
    d. Download data from a personal (non-Council) email account (for example a personal Hotmail account) or external cloud storage provider (for example Google Drive) into Council email or file storage systems.

e. Make official commitments through the internet or email on behalf of the Council unless authorised to do so.

8. Use the internet, email or social media in a way that could affect their reliability or effectiveness, for example distributing chain letters or spam.

9. Download copyrighted material such as eBooks, music media (MP3) files, film and video files, JPEGs, GIFs, or other material without appropriate approval.

10. In any way infringe any copyright, database rights, trademarks, or other intellectual property.

11. Download or install any software from the internet or other sources without prior approval from Customer and Digital Services.

12. Connect Council assets to the internet using non-standard or not approved connections (for example, unsecured Wi-Fi without a password).

If you're unsure in anyway about adhering to the above, please speak to your line manager or contact the Cyber Security Team in Customer and Digital Services.

You should be aware of phishing activities and take steps to prevent them. Unexpected or suspicious emails should not be opened and instructions contained in them should not be followed. Report the email in line with current guidance.

Line managers must ensure individuals are given clear direction on the extent and limits of their authority regarding access to the internet.

Social media use

All communications that individuals make through social media which reference the Council or their role in the Council, must not bring the Council into disrepute, **and must not:**

1. Criticise, disagree, or argue with citizens, service users, colleagues or managers;
2. Make defamatory comments about individuals or other organisations / groups;
3. Contain images that are inappropriate or links to inappropriate content;
4. Agree with or condone inappropriate comments or content;
5. Breach confidentiality, for example by: referring to sensitive or confidential information about an individual (such as a colleague or service user) or the Council.

Individuals must not do anything that could be considered: discriminatory, intimidatory, bullying or harassment, to any individual or group of individuals, and in contravention of the Council's statutory duties, policies or procedures, for example by:

1. Making offensive or derogatory comments relating to groups covered by protected characteristic as detailed in the Equality Act 2010. (See appendix 1 – Legal Provisions).

2. Using social media to bully another individual (such as an employee of the Council).

3. Posting images that are discriminatory, bullying or offensive or links to such content.

4. Agreeing with or condoning inappropriate comments or content that are discriminatory, bullying or offensive.

   The above list is not exhaustive but provides examples illustrating misuse. Individuals are encouraged to talk to their line manager and seek advice if they're unclear.

4. Clear desk, clear screen and secure print

To reduce the risk of unauthorised access or loss of information, the Council enforce a clear desk and screen procedure. Personal or confidential business information must be protected using security features provided.

Individuals must ensure that:

- Devices are logged off or locked or protected with a screen locking mechanism when unattended.
- Steps are taken to ensure computer screens are protected from people looking over their shoulder when confidential information is displayed.
- Passwords or other confidential information used to access computers are not left written down on a desk or screen or are easily accessible by others.
- Other electronic media, for example, authorised USB sticks, are not left unattended at any time.
- Documents are printed using the secure print (PIN required) feature on printers.
- Confidential material is not left unattended on desks, meeting rooms, or on printers or photocopiers.
- All Council related printed matter must be disposed of in confidential waste bins or shredded.
- Workstations are left clear at the end of a working day/shift, including portable ICT devices shut down, removed from the desk and locked away securely.

5. Working Remotely

It's accepted that laptops and mobile devices will be taken off-site to working remotely for business purposes. Working away from the office, including at home, must be in line with the following guidelines.

The following controls must be applied:

1. IT equipment and devices must not be left unattended in public places and must not be left visible in a vehicle, whether Council owned or not.

2. Laptops must be carried as hand luggage when travelling.

3. Steps will be taken to ensure device screens are protected from people looking over your shoulder or nearby CCTV coverage; be aware of who is around you.

4. Take the precaution to protect information against loss or compromise when working remotely; assess your surroundings.

5. Take care when using mobile devices in public places, for example laptops, mobile phones, smartphones, and tablets; assess your surroundings.

6. Mobile devices that hold data must be protected at least by a password or a PIN or alternate approved security methods, and by device encryption.

7. Only connect computers and mobile devices to secure Wi-Fi networks, including home networks. You should refrain from transmitting sensitive or personal or otherwise confidential information via public Wi-Fi, for example in coffee shops or on trains.

8. Only use personal laptops, smartphones, and tablets for Council business once authorisation is obtained from Customer and Digital Services. This may require the installation of specialist device management software to protect the security of our data.

9. Always use computers, mobile devices, and phones safely and in accordance with other legislation, for example do not drive and use a mobile device, comply fully with the provisions of all health and safety guidance and other Council policies and procedures.

10. Printed material must be disposed of by using a cross cut shredder or placed in a confidential waste bag at your work location.

Travel outside the UK

Council ICT equipment must not be taken outside the UK without Customer and Digital Services agreement and in-line with the current National Cyber Security Centre or UK Government guidelines, this is applicable to all Council employees, Councillors**,** contractors, agency workers, volunteers and agents.

Clean devices, not containing data, may have to be provided for the trip. There may be strict requirements about where and when devices are used and what happens to them on return; this will be in line with NCSC guidance at the time of the journey. In some countries government or other agencies may try to obtain information from computers or install malicious software that may not be detectable by standard virus protection.

Advice: If planning a trip outside of the UK, please make sure to engage with Customer and Digital Services early to avoid possible issues at time of travel.

Portable storage devices

Due to the increased possibility of data loss or inappropriate access, care must be taken when using data stored on portable storage devices. Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there's no other secure method of transferring data. Get advice from ICT Solutions before using any devices. The G drive is the Council's primary method of storage - appropriate guidance should be sought from Information Governance if a change to this is required.

Only use Council authorised mobile storage devices with encryption enabled when transferring sensitive or confidential data. Individually purchased memory sticks cannot be used.

If memory sticks are found in the office or in the street they should not be inserted into a Council computer but should be delivered to Cyber Security.

Line managers must ensure individuals are given clear direction on the extent and limits of their authority regarding the use of ICT systems, devices or data away from the office.

6. SOFTWARE USE

Individuals must use only software that is authorised by the Council on authorised computers, smartphones, and tablets when performing Council business.

Procurement and ICT must approve any purchases of IT software or hardware in line with Council standing orders. Authorised software must be used in accordance

with the software supplier's licensing agreements. All software and computer procurement must be obtained through approved channels and installed by ICT Solutions and its IT suppliers.

Individuals must not:

1. Store personal files such as music, video, photographs, or games on our IT equipment.

2. Install unauthorised copies of software, freeware, or shareware on our IT equipment.

3. Install games, music and video streaming, gambling, or shopping applications on our IT devices.

4. Use any software, already installed on our IT equipment, for unauthorised purposes.

Customer and Digital Services, working with our strategic ICT partner, has implemented automated virus, malware, and other detection software to detect and prevent malicious or unwanted activity within the Council. All PCs, laptops and smartphones have such software installed. Individuals must not try to subvert or bypass the operation of this software. Attempts should not be made to remove malware: potentially infected machines should be switched off, disconnected from the network and reported to the ICT Service desk.

7. TELEPHONY (VOICE) EQUIPMENT USE

Our voice equipment is for business use. Individuals must not use our voice facilities for sending or receiving private communications on personal matters, except when agreed with their line manager. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Individuals must not:

1. Use our voice equipment for conducting private business activities.
2. Make hoax or threatening calls to internal or external destinations.
3. Use telephones to breach our policies (for example, Avoidance of bullying and harassment at work policy) or to break the law.
4. Accept reverse charge calls unless authorised or in exceptional circumstances.

Phishing scams by phone

Individuals should be aware of phishing activities initiated by phone or text and take steps to prevent them. Terminate unexpected or suspicious conversations and do not follow requests made during the call. Report any contact of this type in line with current guidance.

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority regarding the use of telephone systems in or away from the office.

8. ACTIONS UPON TERMINATION OF OFFICE / EMPLOYMENT / ENGAGEMENT

At termination of contract all our equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices, CDs and DVDs, must be returned in line with our leavers' process. Where people fail to return devices correctly, then the Council reserves the right to pursue this and to take all appropriate measures, including legal action where necessary.

Individuals leaving our employment should ensure that they know of the behaviours expected of them after they have left in line with other Council policies. For example, accessing or attempting to access data or a Council computer system that they are no longer entitled to use is a criminal offence. Relevant legislation is shown in the Appendix 1 – Legal provisions.

9. REPORTING

It's every individual's responsibility to report suspected breaches of this policy, other security policies and data protection breach procedures immediately to any one of the following:

- Line manager,
- ICT Security,
- Information Governance Unit, within Strategy and Communications,
- The CGI Service desk as a security incident.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action can be taken.

10. APPENDIX 1 – LEGAL PROVISIONS

The Computer Misuse Act 1990 amended by the Police and Justice Act 2006 states that:

- Unauthorised access to computer-based material is punishable by up to two years in prison or a fine or both.

- Unauthorised acts with intent to impair operation of a computer, etc. is punishable by up to 10 years in prison or a fine or both.

For example, it would a criminal offence for an individual to access a Council system just because they knew a colleague's password. This could lead to two years in prison.

The Data Protection Act 1988 and Regulation (EU) 2016/679 (General Data Protection Regulation) sets out what may or may not be done with personal data (that is any information that identifies a living individual).

It states that it is an offence to obtain knowingly or recklessly, disclose, or procure the disclosure of personal information without the consent of the data controller. The offence is punishable by various means and could lead to fines on organisations of up to €20 million or 4% of global annual turnover for the preceding financial year.
For example, it would be contrary to GDPR for an individual to take home a list of citizens' names and address that might be useful to a friend in their plumbing business.

The 1988 Copyright, Designs and Patents Act governs the use of a 'work' created by an individual or company. A "work" is defined as something that is original, created with effort and a tangible entity - an idea cannot be copyright. If a work is produced as part of employment, then the owner will normally be the company that is the employer of the individual who created the work.

It is an offence to perform any of the following acts without the consent of the copyright owner: copy the work; rent, lend the work to the public; broadcast or show the work in public; or adapt the work.

For example, an individual may commit an offence by carrying out the above acts with work they have created while in our employment, e.g. showing documents, they wrote on how to manage Council procurement to a third party. An offence could also be committed with work that is licensed for use in the Council, e.g. copying training material that an individual found useful.

The Equality Act 2010 legally protects people from discrimination in the workplace and in wider society. It replaced previous anti-discrimination laws with a single Act, making the law easier to understand and strengthening protection in some situations. It sets out the different ways in which it is unlawful to treat someone.

The Equality Act 2010 covers the same groups that were protected by existing equality legislation – age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage and civil partnership and pregnancy and maternity.

Other relevant legislation:

• Civil Evidence (Scotland) Act 1988 • Copyright (Computer Programs) Regulations 1992 • Freedom of Information (Scotland) Act 2002 • Human Rights Act 1998 • Counter Terrorism and Security Act (2015); Prevent Guidance	• Official Secrets Act 1989 • Criminal Procedure (Scotland) Act 1995. • Public Records Acts 1958 & 1967 • Regulations of Investigatory Powers (Scotland) Act 2000. • Serious Organised Crime and Police Act 2005	• The Civil Contingencies Act 2004 • The Communications Act 2003 • The Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000 • Wireless Telegraphy Act 2006