Policy and Sustainability Committee

10.00am, Thursday, 10 June 2021

ICT Acceptable Use Policy

Executive/routine	**Executive**
Wards	**All**
Council Commitments	

1. Recommendations

1.1 It is recommended that the Committee approves the updated ICT Acceptable Use Policy for the Council.

Stephen S. Moir

Executive Director of Resources

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

Customer and Digital Services Division, Resources Directorate

E-mail: Nicola.harvey@edinburgh.gov.uk | Tel: 0131 469 5006

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Report

ICT Acceptable Use Policy

2. Executive Summary

2.1 The purpose of this report is to propose an updated policy statement for the ICT Acceptable Use Policy, which was last reviewed and approved by the Committee in May 2019.

2.2 The updated Policy has been developed in line with the best practice guidelines encapsulated in the Scottish Government's Public Sector Cyber Security Action Plan and current advice and best practice from the National Cyber Security Centre.

3. Background

3.1 The ICT Acceptable Use Policy was last revised in May 2019. To ensure that the Council's Policies align with current best practice, legislation and to better defend against emerging and increased cyber-security and serious and organised crime threats to our operations, data and information.

4. Main report

4.1 The information contained in the ICT Acceptable Use Policy is based on guidance as at May 2021. The Policy has been written in line with guidance from the Council's Cyber Security specialists, the Information Governance Unit, 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 will be published on the Council's Intranet site, the Orb, on approval by the Committee.

5.2 Digital Services will ensure that appropriate communications are distributed to all staff affected by the Policy and will embed changes in this within existing security training.

6. Financial impact

6.1 Breaches of cyber security and potentially a breach of the Data Protection Act 2018 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 including compensation for any losses caused.

7. Stakeholder/Community Impact

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

8. Background reading/external references

8.1 City of Edinburgh Council Digital and Smart City Strategy

8.2 Scottish Government Digital Strategy - A Changing Nation: How Scotland Will Thrive In A Digital World

8.3 Cyber Resilient Scotland: Strategic Framework

9. Appendices

9.1 Appendix 1 ICT Acceptable Use Policy

Information and Communications Technology (ICT) Acceptable Use Policy

Implementation date:

Control schedule

Version Control

Version	Date	Author	Comment
0.1	Jan 2019	Neil Dumbleton	Customer and Digital Services Cyber Information Security Steering Group
1.0	May 2019	Neil Dumbleton	Democracy Governance & Resilience
1.1	August 2020	Mike Brown	Review, minor updates to reflect Updated Acts and to reflect new M365 UYOD Standard
1.2	May 2021	Mike Brown	Reviewed and updated to reflect changes to personal email use

Committee decisions affecting this policy

Date	Committee	Link to report	Link to minute
23/05/2019	Finance and Resources	F&R Report - ICT Acceptable Use Policy 2019	F&R Minutes - 23/05/2019

ICT Acceptable Use Policy

Policy statement

1.1 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 and information but to ensure that best practice is followed.

Scope

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

2.2 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.

Definitions

3.1 Information security: ensures that Council information is not compromised by unauthorised access, modification, disclosure or loss.

3.2 Cyber security: ensures that Council information that is processed by computers is not compromised by unauthorised access, modification, disclosure or loss.

Policy content

General Applicability

4.1 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.).

4.2 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.

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

4.4 This policy applies to:

4.4.1 all ‘individuals’ (Council employees, Councillors, contractors, agency workers, volunteers and agents) who use our information and IT equipment;

4.4.2 all information, in whatever form, relating to our business activities worldwide;

4.4.3 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; and,

4.5 Councillors should also abide by the rules surrounding ICT in the Councillors’ Code of Conduct.

4.6 Individuals using the Council’s e-mail system in the performance of authorised trade union duties must also follow any obligations set out in their respective Union privacy policy, as well as the provisions of this policy. Trade union related correspondence transacted on the Council’s e-mail system will be governed by the Trade Union’s data protection responsibilities and the Trade Union concerned will be the data controller for any personal data exchanged.

Misuse of computer equipment

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

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

Monitoring and Controls

4.8 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.

4.9 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.

4.10 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.

4.11 Relevant legislation that applies to the use of Council computer systems is provided.

Changes in Guidance

4.12 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.

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

System Access

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

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

4.16 **Individuals must not:**

- Allow anyone else to use their user ID, token, or password on any Council IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access the Council's IT systems.
- Leave their password unprotected, for example write it down thereby making visible to others.
- Make unauthorised changes to our IT systems or information.
- Attempt to access data that they're not authorised to use or access.
- Exceed the limits of their authority or their specific business need to use the system or data.
- Connect any non-Council authorised device to our network or IT systems.

- Store Council data on any non-authorised Council equipment.

- Give or transfer our data or software to any person or organisation outside the Council without our authority.

- Use computer equipment as a means of breaching our policies or to break the law.

- Look to subvert any IT or other security measures in place.

- Upload unprofessional personal images, football badges, political, celebrity images to systems such as M365 that may allow this functionality. (This list is not exhaustive)

4.17 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.

Internet mail, E-Mail and social media use

4.18 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.

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

4.20 **Individuals must not:**

- Use the internet or email for the purposes of harassing, bullying, abusing, intimidating or victimising individuals or groups.

- 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.

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

- 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.

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

Use the internet, email or social media to:

- make personal gains or conduct a personal business;
- gamble;
- breach any other Council policy; or
- break the law.

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

- Place any information on the internet that relates to the Council or, expresses any opinion about the Council.

- Send personal, sensitive or confidential information externally about any 3rd party without ensuring appropriate encryption is in place.

- Forward Council email or upload data to a personal (non-Council) email account (for example a personal Hotmail account).

- Bypass existing filtering controls to access commercial email and cloud services to 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.

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

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

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

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

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

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

4.21 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.

4.22 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.

4.23 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

4.24 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:**

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

4.25 **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 procedures, for example by:**

- Making offensive or derogatory comments relating to groups covered by protected characteristic as detailed in the Equality Act 2010.
- Using social media to bully another individual (such as an employee of the Council).
- Posting images that are discriminatory, bullying or offensive or links to such content.
- Agreeing with or condoning inappropriate comments or content that are discriminatory, bullying or offensive.

4.26 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.

Clear desk, clear screen and secure print

4.27 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.

4.28 **Individuals must ensure that:**

- Computers 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.

Working Remotely

4.29 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.

4.30 **The following controls must be applied:**

- 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.
- Laptops must be carried as hand luggage when travelling.
- Steps will be taken to ensure device screens are protected from people looking over your shoulder or near CCTV coverage; be aware of who is around you.
- Take the precaution to protect information against loss or compromise when working remotely; assess your surroundings.
- Take care when using mobile devices in public places, for example laptops, mobile phones, smartphones, and tablets; assess your surroundings.
- 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.
- 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.
- 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. Please refer to the Councils UYOD standard for accessing M365 services on personal devices.
- 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.

- 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

4.31 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.

4.32 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.

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

Portable storage devices

4.34 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 Digital Services 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.

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

4.36 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.

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

Software Use

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

4.39 Procurement and Digital Services 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 Digital Services and its IT suppliers.

4.40 **Individuals must not:**

- Store personal files such as music, video, photographs, or games on our IT equipment.
- Install unauthorised copies of software, freeware, or shareware on our IT equipment.
- Install games, music and video streaming, gambling, or shopping applications on our IT devices.
- Use any software, already installed on our IT equipment, for unauthorised purposes.

4.41 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.

4.42 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 IT Service desk.

Telephony (Voice) equipment use

4.43 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.

4.44 **Individuals must not:**

- Use our voice equipment for conducting private business activities.
- Make hoax or threatening calls to internal or external destinations.
- Use telephones to breach our policies (for example, Avoidance of Bullying and Harassment at Work Policy) or to break the law.
- Accept reverse charge calls unless authorised or in exceptional circumstances.

Phishing scams by phone

4.45 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.

4.46 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.

Actions upon termination of office / employment /engagement

4.47 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.

4.48 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 section on related documents).

Reporting

4.49 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:

4.49.1 Line manager;
4.49.2 Cyber (ICT) Security;
4.48.3 Information Governance Unit, within Strategy and Communications; and
4.48.4 The CGI Service desk as a security incident.

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

Implementation

5.1 Implementation of this policy will be supported through continued development and maintenance of security tools and defences.

5.2 Communications awareness campaigns and training will be provided for all 'individuals' (Council employees, Councillors, contractors, agency workers, volunteers and agents) who use our information and IT equipment.

5.3 Progress and performance will be monitored by the Cyber and Information Security Steering Group, chaired by the Executive Director of Resources.

Roles and Responsibilities

6.1 The Policy is prepared by Customer and Digital Services, with contributions from members from the Council's Cyber and Information Security Steering Group

Related documents

Legal Provisions

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

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

7.3 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.

7.4 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.

7.5 **The Data Protection Act 2018** 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).

7.6 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.

7.7 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.

7.8 **The 1988 Copyright, Designs and Patents Act** governs the use of a 'work' created by an individual or company.

7.9 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.

7.10 It's 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.

7.11 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.

7.12 **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's unlawful to treat someone.

7.13 The Equality Act 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.

7.14 Other relevant legislation:

- 7.14.1 Civil Evidence (Scotland) Act 1988
- 7.14.2 Copyright (Computer Programs) Regulations 1992
- 7.14.3 Freedom of Information (Scotland) Act 2002
- 7.14.4 Human Rights Act 1998
- 7.14.5 Counter Terrorism and Border Security Act (2019); Prevent Guidance
- 7.14.6 Official Secrets Act 1989
- 7.14.7 Criminal Procedure (Scotland) Act 1995.
- 7.14.8 Public Records (Scotland) Act 2011
- 7.14.9 Regulations of Investigatory Powers (Scotland) Act 2000.
- 7.14.10 Serious Organised Crime and Police Act 2005
- 7.14.11 The Civil Contingencies Act 2004
- 7.14.12 The Communications Act 2003
- 7.14.13 The Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000
- 7.14.14 Wireless Telegraphy Act 2006

Integrated Impact Assessment

8.1 The integrated impact assessment is being completed in line with Council policy.

Risk assessment

9.1 The principles of information security are underpinned by legislation, and the consequences of a serious breach of information security are severe.

9.2 The risks of not implementing this policy include:

- 9.2.1 Distress or harm to individuals or organisations.
- 9.2.2 Reputational damage to the Council.
- 9.2.3 Financial loss or monetary penalty imposed.
- 9.2.4 Detrimental impact on Council business and service delivery.

Review

10.1 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).