# CORPORATE

# ICT

# ACCEPTABLE USE POLICY

| | | |
|---|---|---|
| **Date:** | 15 May 2019 | |
| **Version:** | V3.0 | |
| **Location:** | Digital and Technology | |
| **Author (s) of Document:** | Lita Greenwell, Information Security Officer | |
| **Approval Authority** | Fraser Bell, Senior Information Risk Owner | |
| **Scheduled Review:** | May 2020 | |
| **Changes:** | September 2017 | Replaces all previous version of ICT & Acceptable Use Policies |
| | April 2019 | Minor updates: reflect organisational change and updates to supporting policies and procedures. |

## 1. What is this policy for?

This policy sets out what is acceptable use of Council Information Communication & Technology (ICT) equipment, systems and networks.

For the avoidance of doubt, this includes, but is not limited to: laptops, notebooks, networks, tablets, desktop computers, mobile telephones, smart phones, telephones, printers, imaging equipment, document centres, tills, kiosks, video conferencing facilities, other peripherals; as well as servers, storage media and systems, power supplies and cabling which is used to deliver ICT and/or voice services to Council staff. “Systems” refers to any Council administered/ hosted/ licensed user accounts, credentials, records and software. Network refers to the infrastructure, and data carried and stored thereon, by Council equipment and systems.

## 2. Who is this policy for?

This policy applies to all staff, agency staff, elected members, contractors and sub-contractors, and to any person, without exception, who uses or requires access to Council owned or leased ICT equipment, systems and networks, as above.

By using any Council ICT equipment, systems and networks, the User agrees to use it in accordance with this Policy as a condition of being provided with access to it.

## 3. Why do we need this policy?

Having in place an ICT Acceptable Use Policy provides Users with clear information about their responsibilities when using Council ICT equipment, systems and networks.

This means all Users have a shared understanding of what acceptable use is, and are confident in using ICT equipment, systems and networks in line with the Council’s values and behaviours, and in accordance with the Employee Code of Conduct (for Council Employees), and The Elected Member Code of Conduct (for Elected Members), and in accordance with the terms of this Policy.

Making sure that the Council has a clear Policy in place for the Acceptable Use of ICT equipment, systems and networks will mean that the Council complies with relevant legislation, regulatory codes of practice, and our own corporate governance requirements.

## 4. What does it mean for the Council? (Policy Statement)

### 4.1 Acceptable Use

The Council defines acceptable use as the use of Council ICT equipment, systems and networks in support of carrying out its business and/or functions, or any other permitted activity highlighted by this Policy. This includes official trade union business, Council sponsored training or educational courses, and limited personal use. The following criteria will be used, where relevant, to assess whether usage is acceptable:

- whether usage is in support of business and service needs consistent with Council policies;
- whether usage is in support of an individual's approved duties/remit;
- whether usage is consistent with the Council policy, procedure and guidance that is appropriate to any system or network being used/accessed;
- whether the handling of the information is appropriate for the type of information; and
- whether usage is limited personal use as defined in 4.2 Personal Use of Council ICT.

Any questions or guidance about acceptable usage should be discussed with the User's Line Manager.

### 4.2 Personal Use of Council ICT Equipment, Systems and Networks

ICT equipment and services may be used for limited personal usage provided that:

- this is not associated with monetary reward;
- it is undertaken in the user's own time (non-work hours e.g. lunch break, before or after work);
- it does not interfere with the delivery of Council services; and
- it does not violate this or any other Council policy, and is a lawful activity.

Where the Council's email system is used to send a personal email, only the words 'PERSONAL EMAIL' should appear in the subject field of an email. This is intended to ensure that the content of such messages is not reported on as part of the Council's Electronic Monitoring of Users' email.

Any questions or guidance about acceptable Personal Use of the Council's ICT equipment, systems and networks should be discussed with the User's Line Manager.

The Council accepts no liability for any loss or detriment suffered by personal use of Council ICT equipment, systems and networks. The Council does not provide a secure transaction system for any information passed, or purchase made, for personal use. Any personal use of Council ICT equipment, systems and networks to create, send, import or store personal information is done entirely at the User's own risk.

### 4.3 Security

All Users must:

- not share their account passwords or allow another person to use their account(s);
- not use or attempt to use another individual's account(s);
- make sure that passwords used to protect network access, systems and applications are maintained securely, and comply with current guidelines;
- not leave unattended ICT equipment logged on without first locking the device (if a lock facility is not available then the user must log out);

- notify the ICT Service Desk and their line manager if they suspect or identify a security problem or a breach of the ICT Acceptable Use Policy by any user, in line with the Information Security Incident Reporting Procedure;
- take reasonable precautions to protect the Council's ICT equipment, systems and networks from security issues such as computer viruses and malware. To reduce the risk of potential viruses and malware, users should not open any suspicious email attachments or independently load any software, including screensavers, onto their computers. If a user does inadvertently open a message or attachment that contains a virus or malware, they should contact the ICT Service Desk immediately;
- use only properly supplied and authorised systems for undertaking Council business; and
- use only authorised software to access the internet.

### 4.4 Unacceptable Use

The effective operation of the Council's ICT equipment, systems and networks relies heavily on the proper conduct of all Users. The use of all ICT equipment, systems and networks must be in compliance with all appropriate legislation, relevant Codes of Conduct and Council Policies.

Users must only use ICT equipment, systems or networks that have been authorised for their use. Any attempt to gain unauthorised access to any ICT equipment, systems or networks provided by the Council, or use of the Council's ICT equipment, systems or networks to gain unauthorised access to any other system may be a breach of this policy, and may also be a breach of legislation (including the Computer Misuse Act 1990). Only hardware and software that has been authorised for use by ICT Services are acceptable for Internet and E-mail access use.

For a list of examples of unacceptable uses of Council ICT equipment, systems and networks please refer to **Appendix 1** of this Policy. Users should note that this is not an exhaustive list, and each potential breach of this Policy will be assessed on its individual circumstances. If a User is in any doubt about what constitutes acceptable or unacceptable use they should seek clarification from their Line Manager in the first instance.

### 4.5 Email

Email needs to be constructed with the same regard for the rules applicable to other forms of business communication, as it can be considered binding in business transactions, as well as being admissible evidence in court.

Confidential or otherwise sensitive information must be appropriately protected at all times. When emailing sensitive information outside the Council Users must ensure that either the email transmission is encrypted, the information itself is encrypted (by password protecting an attached document) or both. If you need advice or assistance please contact your Line Manager or the IT Service Desk. Non Council email accounts must not be used to conduct council business unless a User has been authorised to do so.

Users who wish to communicate confidential, work-related information to their Trades Union or relevant Council Service should prefix their email message

descriptions with the words 'PRIVATE EMAIL' and then add subject-specific wording as per the following examples:

- PRIVATE EMAIL – UNISON;
- PRIVATE EMAIL – HEALTH MATTER
- PRIVATE EMAIL – EMPLOYEE PENSION etc.

This is intended to ensure that the content of such messages is not reported on as part of the Council's electronic monitoring of Users' email.

### 4.6 System Back-ups

Any personal information that Users enter on any Council ICT equipment, systems and networks will, in general, be handled in the same way as business information. For example, data on the Council's main networks and transaction logs are routinely backed up by either the Council or our service supplier, and will be stored for a period of time**.**

### 4.7 Access

It may sometimes prove necessary for ICT systems to be accessed by the Council's management, nominated representatives and/or the Police (in particular circumstances), and for the contents of a User's ICT accounts to be examined. The Council reserves the right to do this. Access to Users accounts will be managed in accordance with the Requesting Access to Information Procedure.

### 4.8 Monitoring

The Council seeks to safeguard Users of its ICT equipment, systems and networks from inappropriate activities and unacceptable material. One of its safeguards is monitoring, others include a suite of defensive measures at the perimeter and within the network. All Council ICT equipment, systems and networks may be monitored for compliance with current legislation and Council policies. Monitoring also has the following purposes:

- to establish compliance with Council policies;
- to investigate any suspected or actual breaches of Council policy;
- to investigate system performance;
- to gather evidence for investigative or disciplinary purposes; and
- for other legal and security purposes.

Monitoring is undertaken in accordance with the Council's approved Corporate Protective Monitoring Policy

### 4.9 Breaches and Incidents Reporting

All Users are responsible for reporting known or suspected breaches of this Policy immediately to their Line Manager and the ICT Service Desk, in line with the Information Security Incident Reporting Procedure.

### 4.10 Consequences of Misuse

The Council may, at its sole discretion, suspend or terminate ICT access, withdraw or remove any material uploaded by the User in contravention of this Policy. The Council may take such action as it considers necessary, including taking disciplinary action or disclosing information to law enforcement agencies.

Any other Users that are not employed by the Council and not subject to the Council disciplinary procedure will be subject to provisions in the contract held with them or other acceptable use agreement they have entered into. In any event, misuse may result in the withdrawal of ICT access or equipment, legal action or the involvement of law enforcement agencies.

Users should be aware that use of Council ICT equipment, systems and networks may be monitored at all times and monitoring information is retained and used for both routine monitoring reports and to support potential misuse reports.

## 5. How will we know if it's working?

All activity relating to this policy will be reported by the Council's Senior Information Risk Owner (SIRO) to the Corporate Management Team, as required.

## 6. How will we manage any risks that affect this policy?

### 6.1 Cluster Risk Registers

Information Asset Owners are responsible for managing risk to the information assets that they are responsible for; these risks are managed through Cluster Risk Registers and are included in Business Continuity planning and disaster recovery arrangements wherever appropriate.

### 6.2 Corporate Risk Register

**Information Governance and Cyber Security also pose a strategic risk for the Council. The relevant Corporate Risk Owners provide the Council's Corporate Management Team with regular updates on the strength of controls in place against this risk.** **7. How will we make sure this policy is kept up to date?**

This Policy will be reviewed annually by the Council's Information Security Officer to ensure that it meets business and accountability requirements and measurable standards of good practice.

## 8. Related Policy Document Suite

- Corporate Information Policy
- ICT Access Control Policy
- Employee Code of Conduct (for Employees only)
- Councillors Code of Conduct (for Elected Members only)

**Procedure**

- Corporate Information Handbook
- Information Security Incident Reporting Procedure
- Requesting Access to Information Procedure
- Information Asset Owner Handbook
- Guidance on the Use by Employees of the Council's Telephone Systems for Private Calls and of Mobile Devices for Private Calls and Digital Messaging

**Related Legislation**

- The Data Protection Act (2018)
- General Data Protection Regulation
- The Freedom of Information (Scotland) Act 2002
- The Public Records (Scotland) Act 2011
- The Environmental Information (Scotland) Regulation 2004
- The Computer Misuse Act (1990)
- The Copyright, Designs and Patents Act (1988)
- The Health & Safety at Work Act (1974)
- The Human Rights Act (1998)
- The Regulation of Investigatory Powers (Scotland) Act 2000

## Appendix One: Examples of Unacceptable Use

It is unacceptable for a User to use, submit, publish, display, download or transmit (including the sharing of links) on or from the network or on any Council ICT system or device which connects to the Council network or is operated by the Council (or our ICT providers) any information or material which:

- restricts or inhibits other Users from using the system or impairs the efficiency of the ICT systems;
- violates or infringes upon the rights of any other person, including the right to privacy;
- is offensive, indecent or obscene or abusive images and literature, including images containing nudity or sexually explicit content;
- can reasonably be considered to promote any form of deception, defamation, discrimination, harassment, maliciousness, misrepresentation, racism, victimisation, intolerance or violence;
- encourages the use of controlled substances or uses the system with criminal intent;
- uses the system for any other illegal purpose; and
- breaches legislation or statutory requirements which the Council has to comply with e.g. Data Protection Act 1998, Copyright Designs & Patents Act 1988.

It is unacceptable for a User to use the facilities and capabilities of the Council's ICT systems to:

- conduct any non-approved business;
- download or install any unauthorised software;
- undertake any activities detrimental to the reputation of the Council;
- transmit material, information or software in violation of any local, national or international law;
- undertake, plan or encourage any illegal purpose;
- deliberately contribute to websites that advocate illegal activity;
- harass an individual or group of individuals;
- make offensive or derogatory remarks about anybody on social media and discussion forums;
- post offensive, obscene or derogatory content (including photographs, images, commentary, videos or audio) on social media and discussion forums;
- create or share any content which breaches confidentiality;
- transmit spam (electronic junk mail) or chain email;
- attempt to compromise Council ICT equipment, systems and networks, prevent legitimate access to them, damage them or seek to cause degradation of performance or a denial of service;
- view, transmit, copy, download or produce material, including (but not exhaustively) software, films, television programmes, music, electronic documents and books which infringes the copyright of another person, or organisation;
- conduct any unauthorised political activity;

- conduct any non-Council approved fund raising or non-Council related public relations activities;
- conduct commercial activities which are not connected to Council business, including but not limited to activities in connection with outside offices or employment, or self-employment ;
- undertake any form of gaming, lottery or betting;
- undertake any form of share dealing;
- offer items for sale, or place bids on, commercial auction sites (such as eBay™);
- participate in Chain Schemes (such as pyramid selling);
- access or transmit information via the Internet, including email, in an attempt to impersonate another individual;
- attempt to gain deliberate access to facilities or services which a User is unauthorised to access;
- attempt to bypass the Council internet filtering or any ICT monitoring functions;
- deliberately undertake activities that corrupt or destroy other Users' data; disrupt the work of other Users, or deny network resources to them; violate the privacy of other Users;
- send sensitive personal data by email to unsecure external email addresses/contacts (unless a secure method is used, for example password protecting the document);
- attempt to gain unauthorized access to Council ICT equipment, systems and networks or content for which you do not have permission (i.e. Hacking);
- attempt to access, amend, damage, delete or disseminate another User's files, emails, communications or data without the appropriate authority;
- where Users are authorised to access the Council's main email system over the Internet, using non-Council computers and services, they must not access messages or attachments which they know or suspect contain confidential or otherwise sensitive information;
- make any unauthorised alteration to the standard device configuration or image (except for the user customisation options found within operating systems, e.g. themes, sounds, desktop wallpaper); and
- download or install any software or scripts which have not been cleared through the standard procedure.

This list represents examples of unacceptable use, but this is not an exhaustive list. Each potential breach of this policy will be assessed on its individual circumstances. If a User is in any doubt about what constitutes acceptable or unacceptable use they should seek clarification from their Line Manager in the first instance.