CORPORATE POLICY

ICT

ACCEPTABLE USE POLICY

Date:	15 September 2015	
Version:	V1.0	
Location:	IT & Transformation	
Author (s) of Document:	Caroline Anderson, Information Manager	
Approval Authority	Finance, Policy & Resources	
Scheduled Review:	15 September 2016	
Changes:	15 September 2015	Replaces all previous version of IT & Telecommunications Acceptable Use Policies

What is this policy for?

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

Who is this policy for?

This policy applies to everyone who uses Council owned or leased of Council ICT equipment, systems and networks; including, but not limited to: computers, laptops, tablets, notebooks, smart phones, computer kiosks, printers, fax machines, photocopiers, document centres, video conference facilities and telephones.

Why do we need this policy?

Having in place an ICT Acceptable Use Policy provides Users with their clear and easily understandable 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, as embodied in our Code of Conduct and core corporate behaviours of respect, professionalism, customer focus, communication, leadership, future focus, engagement and creative thinking.

This allows the Council to improve the experience for our staff, as we foster an environment where we trust our staff to use Council resources appropriately.

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.

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

The Council defines 'Acceptable Use', as the use of ICT equipment, systems and networks in support of official core business, 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 Council defines 'Unacceptable Use' as knowingly using ICT equipment, systems and networks to:

- Access, store or transmit offensive, indecent or obscene material or abusive images and literature;
- Access, store or transmit material which can reasonably be considered to promote any form of deception, defamation, discrimination, harassment, maliciousness, misrepresentation, racism, victimisation, intolerance or violence;

- Access, store or transmit material obtained in violation of copyright or used in breach of a licence agreement;
- Transmit spam (electronic junk mail) or chain email;
- Store or transmit material that could reasonably be expected to embarrass or compromise the Council;
- Conduct commercial activities which are not connected to Council business;
- 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);
- Create, store or send material designed to mislead people about who originated or authorised it (e.g. through misuse of scanned signatures);
- 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;
- Log on with the specific purpose of enabling another to then access Council ICT equipment, systems and networks with that account, impersonate others or use another person's login;
- 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;
- Sending confidential or otherwise sensitive information over the Internet, it must be always be contained in a password-protected attachment – with the intended recipient being advised separately of what the related password is;
- Use your Government Connect Secure eXtranet (GCSX) email or its address for any personal use.

Any Unacceptable Use may result in disciplinary action, and possibly prosecution.

Passwords

Passwords must be used to protect all network access, systems and applications and must be maintained securely, not disclosed to others and comply with current guidelines.

Personal Use of Council ICT equipment, systems and networks

The Council does not impose a blanket ban on personal use (this means any use that is not part of Council business or an individual's official duties) of Council ICT.

However, personal use may be withdrawn for operational reasons, or if misused, and must not:

- be unacceptable as defined by this policy
- involve storage or transmission of large amounts of data
- interfere with your official duties

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 Users own risk.

System Back-ups, Access and Monitoring

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. It may sometimes prove necessary for 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.

Breaches and Incidents Reporting

All users are responsible for reporting known or suspected breaches of this Policy immediately to their Line Manager, who should then report the incident to the ICT helpdesk in the first instance.

How will we make it happen?

The Council seeks to safeguard users of its 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
- for other legal and security purposes

Any personal information collected during monitoring will only be used for the purposes for which it was collected, except where it reveals information that the Council could not reasonably ignore (e.g. evidence of gross misconduct). Monitoring is not conducted for the purposes of establishing performance or efficiency of

employees (except where local agreements have been negotiated which rely on agreed automated performance measures).

How will we know if it's working?

All activity relating to this policy will be reported by the SIRO to the Corporate Management Team, as required.

How will we make sure this policy is kept up to date?

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

Related Policy Document Suite

Policy and Strategy

- Data Protection Policy
- Information Management Strategy
- Employee Code of Conduct
- Financial Regulations
- Information Security Policy

Guidelines

- 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
- Corporate Information Security Standards (under development)

Tools

- Information Lifecycle Management Toolkit (under development)

Related Legislation and Supporting Documents

- The Data Protection Act (1998)
- 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