

Corporate Policy and Strategy Committee

10.00am, Tuesday 25 February 2014

ICT Acceptable Use Policy

Item number	7.6
Report number	
Wards	None

Links

Coalition pledges	P27
Council outcomes	CO24, CO26, CO27
Single Outcome Agreement	SO1

Alastair Maclean

Director of Corporate Governance

Contact: Philip Barr, Head of Organisational Development

E-mail: philip.barr@edinburgh.gov.uk | Tel: 0131 469 3963

Executive summary

ICT Acceptable Use Policy

Summary

The Council has an existing policy which covers employees' use of information and communication technology (ICT). The Code of Conduct on the use of Electronic Communications is a Local Collective Agreement covering all staff and was agreed on 15 January 2002. The policy was agreed prior to the growth in the use of mobile information technology, such as smart phones, iPads and other hand held devices and social media sites, such as Facebook, Twitter, blogs, LinkedIn, forums and podcasts.

The new ICT Acceptable Use Policy reflects these and other changes and clarifies the Council's expected standards of behaviour in relation to staff who use ICT at work or at home. It will replace the 2002 policy.

The new Policy is part of the regulatory suite of policies and will be incorporated into the Council's induction and mandatory training programme.

Recommendations

The Corporate Policy and Strategy Committee are recommended to:

- 1) note the contents of this report; and
- 2) approve the revised ICT Acceptable Use Policy for implementation.

Measures of success

- Staff have a better understanding of the standards of behaviour expected of them when using ICT.
- Clarity for managers and staff of acceptable and unacceptable use of ICT resulting in a reduction in incidents of inappropriate use.
- Staff are confident to use ICT to develop and support new ways of delivering services to further the Council's objectives.

Financial impact

- No overall adverse financial implications for the Council.

Equalities impact

- There are no adverse equality issues arising from this report which will impact on employee groups with protected characteristics as defined by the Equality Act 2010. The equality relevance assessment score is 0.

Sustainability impact

- No impact.

Consultation and engagement

- Consultation took place with ICT colleagues to make sure the new policy is up-to-date and as future proofed as possible. Advice was sought from independent experts (Gartner) to ensure that we are adopting good practice and are benchmarking against leading specialists.
- A series of consultation meetings was held with the Trade Unions during December 2013 and January 2014. The policy was confirmed as a Local Collective Agreement on 15 January 2014.

Background reading / external references

- None.

ICT Acceptable Use Policy

1. Background

- 1.1 The Council's existing policy on information and communication technology (ICT) is called the Code of Conduct on the Use of Electronic Communications. It was agreed with the Trade Unions in January 2002 and, as a result, does not reflect the growth in the use of mobile technology and social media in the last 12 years.
- 1.2 ICT has developed significantly in the last decade and the Council is embracing the opportunities offered by ICT for delivering services, enhancing engagement and communicating with staff, service users, the media and the general public.
- 1.3 It is essential that our employment policies reflect technological and social developments. The new ICT Acceptable Use Policy meets that requirement.
- 1.4 The Trade Unions have confirmed the ICT Acceptable Use Policy as Local Collective Agreement.
- 1.5 The Policy is part of the regulatory suite of policies and will be incorporated into the Council's induction and mandatory training programme.

2. Main report

- 2.1 Effective use of technology enhances the Council's efficiency and reputation, providing opportunities to communicate internally, with partners and with the public. The use of electronic equipment, technology and information carries certain risks which can affect the Council in terms of legal liability, reputation and business effectiveness. Using mobile ICT technologies such as smart phones and tablets and online services such as social media introduces additional risks and hazards.
- 2.2 To maximise the benefits, manage the risks and protect the Council and its employees, the ICT Acceptable Use Policy outlines the standards of conduct that are required of all staff when using all electronic communications and systems. Appropriate monitoring arrangements will help make sure that these standards of conduct are met.
- 2.3 This policy applies to all City of Edinburgh Council employees whether or not they are provided with or use Council ICT systems. Agency staff working in the Council and other contractors and consultants will also be required to comply with the principles outlined in the policy while they are working for the Council.
- 2.4 The Policy contains a revised definition of 'Council ICT systems' which includes mobile phones, multimedia devices, PCs, laptop computers, tablets, faxes and

any other forms of electronic information/communication equipment. It applies to any personal or electronic information/communication equipment that an employee uses in the course of their employment.

- 2.5 Social networking sites carry particular risks because they are public. Some Council employees will be given access to social networking sites and this will be agreed by managers on the basis of business need. The Policy makes clear that, unless they have permission from the Council's Web and New Media Board, staff must not post (publish) any information as a representative of the Council.
- 2.6 The Policy also covers activity on a personal basis, whether at work or outside work. If an employee of the Council makes an electronic comment on the internet (blogs, social media, twitter etc.) they must comply with the Council's standards of conduct and behaviour. Failure to do so may result in disciplinary action up to and including dismissal and, in some cases, may be a criminal offence.
- 2.7 The Policy sets out clear Standards of Conduct that staff are expected to follow. It also sets out (in Appendix 1 to the Policy) examples of activity or behaviour that is likely to be treated as unacceptable under this Policy. A toolkit has been developed to provide additional guidance for staff and managers.
- 2.8 It is intended to continue with the established practice of developing joint implementation arrangements with the Trade Union Side.

3. Recommendations

- 3.1 The Corporate Policy and Strategy Committee are recommended to:
 - 3.1.1 note the contents of this report; and
 - 3.1.2 approve the revised ICT Acceptable Use Policy for implementation.

Alastair Maclean

Director of Corporate Governance

Links

Coalition pledges	P27 - Seek to work in full partnership with Council staff and their representatives
Council outcomes	CO24 - The Council communicates effectively and internally and externally and has an excellent reputation for customer care CO26 - The Council engages with stakeholders and works in partnership to improve services and deliver on agreed objectives. CO27 - The Council supports, invests in and develops our people

**Single Outcome
Agreement
Appendices**

SO1

1. ICT Acceptable Use Policy

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) ACCEPTABLE USE POLICY

(covering all employees, agency staff, consultants & contractors)

Contents

1.	INTRODUCTION	2
2.	SCOPE	2
3.	DEFINITIONS	2
4.	STANDARDS OF CONDUCT - GENERAL USE OF COUNCIL ICT SYSTEMS	2
5.	STANDARDS OF CONDUCT - PERSONAL USE OF COUNCIL ICT SYSTEMS	4
6.	STANDARDS OF CONDUCT - USE OF SOCIAL MEDIA	5
7.	MONITORING	5
8.	FAILURE TO FOLLOW THE STANDARDS OF CONDUCT	6
9.	LOCAL COLLECTIVE AGREEMENT	6
	Appendix 1 – Unacceptable Use of Council ICT Systems	7
	Appendix 2 – Roles and Responsibilities	9

15 January 2014
Amended 12 February 2014

1. INTRODUCTION

- 1.1 Effective use of technology enhances the Council's efficiency and reputation, providing opportunities to communicate and interact internally, with partners and with the public. The use of electronic equipment, technology and information carries certain risks which can affect the Council in terms of legal liability, reputation and business effectiveness.
- 1.2 To maximise the benefits, manage the risks and protect the Council and its employees, this Policy outlines the standards of conduct that are required of you when using all electronic communications and systems. There are some helpful factsheets on the Orb for guidance on Do's and Don'ts when using Council ICT Systems. [insert link](#)

2. SCOPE

- 2.1 This policy applies to all City of Edinburgh Council employees **whether or not you are** provided with or use Council ICT systems.
- 2.2 Agency staff working in the Council, consultants and contractors will be required to comply with the principles outlined in this policy while they are working for the Council. Any issues of concern or where potential misconduct is identified will be dealt with under their respective organisations' employment policies and/or the contract.

3. DEFINITIONS

- 3.1 **Electronic equipment and technology** includes all computer and telephone equipment including mobile phones, multi media devices, PC's, laptop computers, tablets, faxes, and any other form of electronic equipment. It also applies to any **personal electronic equipment** or technology that an employee uses in the course of their employment. The Council's electronic equipment and technology will be referred to as "Council ICT systems."
- 3.2 **Electronic communications** include e-mail, text messages, instant messaging, images, fax messages, phone calls and messages, intranet and internet content/messages including social media sites.
- 3.3 **Social Media** includes websites and online tools that allow users to share content, express opinions or interact with each other e.g. Facebook, Twitter, LinkedIn, forums, blogs, podcasts and content communities e.g. YouTube, Flickr, Knowledge Hub.
- 3.4 **Data** includes any electronic or paper information stored or processed on Council networks or equipment including documents, pictures and/or photographs, music and/or video clips.

These definitions are not exhaustive.

4. STANDARDS OF CONDUCT – GENERAL USE OF COUNCIL ICT SYSTEMS

- 4.1 Any information created or held on Council ICT systems will be considered to be owned by the Council. You should not consider any electronic information to be private if it has been created or stored on Council ICT systems. This includes e-mail and internet communications.
- 4.2 You must make sure that you communicate in a way that supports the Council's Policy on equalities. You should therefore make sure that you **do not** send/upload/post information on-line which:
- damages the Council's reputation or undermines public confidence in the Council;
 - supports Political activity (other than any required in your role);
 - includes any libellous or defamatory material about any individual, firm, body or organisation; or
 - harasses, bullies or stalks another person.
- 4.3 You should not use personal electronic equipment and technology for work unless you have permission from your manager. If permission has been given the standards of conduct in this policy will apply to your personal equipment when you are using it for work purposes.
- 4.4 If you make an electronic comment on the internet (blogs, social media, twitter etc.) on a personal basis you must be aware that, as an employee of the Council you are expected to comply with the standards of conduct and behaviour in this policy, the Employee Code of Conduct and the Disciplinary Code. [insert links](#)
- 4.5 You must not claim to represent the views of the Council unless you have permission to do so as part of your job. Similarly, you must not try and pass off your own comments or views as being from someone else by, for example, falsifying your email address or using someone else's.
- 4.6 You must not use social media, the internet, intranet, media, or social media sites to make complaints about your employment. If you want to make a complaint about any aspect of your employment with the Council you must use the appropriate employment procedure (e.g. Grievance, Fair Treatment at Work, Public Interest Disclosure/Whistleblowing).[insert links](#)
- 4.7 Data which involves images of people is covered by strict rules which prevent the use of sensitive data on children and vulnerable adults. You should therefore check any available guidance relating to your job and work area before using this type of data.
- 4.8 You must make sure that any data stored and/or processed using Council ICT systems complies with the laws on data protection and copyright, is shared only with the intended recipient(s) and only when permission has been given or the information is already widely in the public domain.

- 4.9 You must not email, upload or post confidential or sensitive data relating to individuals, partner organisations or any aspect of the Council's business on the internet or the Orb, or remove it from Council property without permission from your manager.
- 4.10 You must maintain security of information by, for example, logging off. Accidental disclosure of personal information can occur if unattended computers are left logged on to systems or a computer printout is not shredded prior to disposal. You should not leave any mobile equipment unattended unless it is absolutely necessary and if you do so you must ensure that it is secure and protected from risk of theft or use by others.
- 4.11 You must keep your password(s) confidential (don't share them with anyone else) and comply with password security arrangements.
- 4.12 You should not try to use or access any part of the Council's ICT systems, data or networks which you do not have permission to access or deliberately do anything which would disrupt or damage them in any way.
- 4.13 You must not process or store Council information on non-Council equipment unless you have permission from your manager or you are using an ICT service which has been approved by the ICT Solutions Team.
- 4.14 You must not download or install any software, hardware or other devices to Council ICT systems or equipment unless you have permission from your manager. This includes 'free' software, screensavers and games.
- 4.15 It is a criminal offence to use a mobile device whilst driving and a conviction will attract a fixed penalty and a license endorsement. If you are caught driving while using a mobile phone or device you may be subject to disciplinary action and will be responsible for the payment any fines/penalties imposed on you.

5. STANDARDS OF CONDUCT - PERSONAL USE OF COUNCIL ICT SYSTEMS

- 5.1 Personal use of Council ICT systems will be permitted on a limited basis, subject to the standards of conduct outlined in this policy. The Council reserves the right to restrict personal use of its ICT systems.
- 5.2 Personal use of Council e-mail and telephones: It is accepted that you may occasionally need to use Council systems to make a private call or email during working time but these should be kept to a minimum. Private calls/emails/texts must, wherever possible, be conducted in your own time. (This also applies to private calls/emails/texts using your own personal equipment during working time).
- 5.3 Personal calls/text messages on Council-owned telephones: The Council can charge you for the cost of these. The Council reserves the right to charge for personal use of any other ICT systems provided for business use.
- 5.4 Personal use of the internet: This is **only** permitted in your own time i.e. outside normal working hours or any additional working hours approved by your line manager. If you clock in and out under the Council's 'flexitime scheme' (Scheme

of Flexible Working Hours) you must be 'clocked out' of the system before using the internet for personal purposes.

- 5.5 Personal use of social media sites: The Council will determine which social media sites may be accessed by staff for personal use. Some sites may not be accessed on ICT systems and these will appear as 'blocked' on your screen.
- 5.6 Any personal use of Council ICT systems must not expose the Council's security, systems or data to risk. You must not:
- circulate non-business e-mails;
 - allow non-Council employees (including family members) to use Council equipment; or
 - attach any personal equipment to Council ICT systems without the approval of the ICT Solutions Team.
- 5.7 You must not access personal web mail accounts, such as those on yahoo, MSN, blueyonder, gmail or hotmail, on Council ICT Systems. These sites are not protected by the Council's security systems and accessing them will put the Council's ICT systems at risk of virus attacks.
- 5.8 You must not knowingly access or try to access inappropriate internet sites, materials or downloads. Pornographic, illegal or other sites which would breach the Council's Employee Code of Conduct, Disciplinary Code or equality standards, must not be accessed from Council ICT Systems or from personal equipment when it is used for work purposes or in work time.

6. STANDARDS OF CONDUCT - USE OF SOCIAL MEDIA

- 6.1 Your manager will decide if you need access to social media sites to carry out your duties at work and you will be given access to them. In order to access them you will have a personal social media account. When you are using social media you must behave in accordance with the standards set out in this policy.
- 6.2 When using social media sites you must not publish or post any information that you have received or have access to as a result of your employment as this is confidential to your work.
- 6.3 You must not use social media sites in any way that may undermine public confidence in the Council, bring the Council into disrepute, or would be discriminatory or defamatory e.g. publish or post any information including comments, jokes, illegal or prohibited images or other materials which would put the Council at risk of legal action being taken against it.
- 6.4 You should avoid informal personal contact with pupils or service users you work with directly, or their carers, through social media sites (e.g. do not add them as a 'friend', 'follow' them or link with them), or using your own personal electronic equipment (e.g. email, text, calls).
- 6.5 You must not use social media to harass, bully, stalk or behave in any other way that could damage your working relationships with your colleagues, members of the public or elected members.

7. MONITORING

- 7.1 The Council will monitor the use of its systems to measure system security, performance, whether employees are meeting the standards of conduct in this policy and for the prevention and detection of crime.
- 7.2 The Council will monitor and log all intranet/internet service traffic and e-mail activity, and reserves the right to access, retrieve and delete:
- all e-mail including in draft form, sent or received;
 - all e-mail boxes and private directories;
 - all use of intra/internet and other communication techniques using the Council's ICT systems e.g. Twitter, blogs etc; and
 - all screensavers, software, materials etc.
- 7.3 Use of the Council's telephone, fax systems and mobile telephones will also be monitored and logged and may be recorded.
- 7.4 The Regulation of Investigatory Powers Act 2000 sets out the circumstances when it is legal for an organisation to monitor or record communications when they enter, or are being sent within, the organisation's ICT systems. These are where:
- the employer reasonably believes that the sender and person intended to receive it have consented to the interception; and/or
 - the employer may monitor without consent in certain circumstances, for example, to prevent crime, protect their business or to comply with financial regulations.

The Act applies to public and private communication networks. It gives the person who sends or receives a communication the right to claim damages against the organisation for the unlawful interception of communications.

8. FAILURE TO FOLLOW THE STANDARDS OF CONDUCT

If you fail to follow the standards of conduct set out in this policy (see sections 4, 5 and 6), use of the Council's ICT systems may be withdrawn from you and/or disciplinary action taken against you, up to and including dismissal. Appendix 1 gives some examples of activity and behaviour which may be considered unacceptable.

9. LOCAL COLLECTIVE AGREEMENT

This policy is a local collective agreement between the Council and the recognised trade unions. Every effort will be made by both parties to make sure that this policy is reviewed regularly and amended by agreement, if required to meet future needs. In the event of a failure to reach agreement both parties reserve the right to end this local agreement by giving four months notice in writing. In such circumstances the terms of the local agreement will no longer apply to existing and future employees.

UNACCEPTABLE USE OF COUNCIL ICT SYSTEMS

1. This Appendix gives some examples of activity and behaviour which may be considered to be unacceptable use of Council ICT systems. The behaviours and activities described below may affect whether you can continue in your job and may also result in disciplinary action being taken against you which can include dismissal from your post.
2. In certain circumstances failure to follow the standards of conduct may also be unlawful, and your activities may be reported to the police and may result in criminal proceedings against you.
3. Certain jobs are also governed by external registration requirements and professional standards of conduct. The Council is required to notify certain external registration bodies of any misconduct by and/or disciplinary action taken against staff.

Examples of Unacceptable Activity and Behaviour

Personal Behaviour

- ✘ Using working time to send personal e-mails, telephone calls or text messages over and above the limited use described in paragraph 5.2 of the policy.
- ✘ Accessing the internet for personal use during working time.
- ✘ Circulating non-business e-mails.
- ✘ Allowing people not employed by the Council (including family members) to use Council equipment.
- ✘ Harassing, bullying or stalking another person online.
- ✘ Sending any material that is discriminatory or damaging to others such as jokes, comments, pictures or other material.
- ✘ Knowingly accessing or trying to access inappropriate internet sites, materials or downloads such as pornographic, illegal or other sites. This applies to Council ICT Systems and to your own personal electronic equipment and technology when it is used for work purposes or in working time.
- ✘ Sending, uploading, posting or publishing online any information or comment about an individual, company or organisation which is defamatory or libellous.
- ✘ Connecting or linking with service users, their carers or pupils that you work with on social media sites (such as Facebook, LinkedIn etc.).
- ✘ Using a mobile device while driving.

Security

- ✘ Sharing your password(s) or failing to comply with other security arrangements.
- ✘ Attaching any personal equipment to Council ICT systems without the approval of the ICT Solutions Team.

- ✘ Using your own electronic and technological equipment for work without permission.
- ✘ Accessing personal web mail accounts, such as those on yahoo, MSN, blueyonder, gmail or hotmail, on Council ICT Systems. (These sites are not protected by the Council's security systems and accessing them will put the Council's ICT systems at risk of virus attacks).
- ✘ Downloading or installing software, hardware etc onto ICT systems without permission.
- ✘ Trying to access a part of the Council's ICT systems which you do not have permission to access or deliberately trying to damage or disrupt them.

Public Activity

- ✘ Making public information that you have received or have access to as part of your employment – this is confidential to the Council.
- ✘ Giving information to the media if you are not authorised to do so by your manager.
- ✘ Posting (publishing) any information on the internet or social media sites as a representative of the Council unless you have permission from the Council Web and New Media Board.
- ✘ Claiming that you represent the views of the Council without permission from your manager.
- ✘ Making public any information which may undermine confidence in the Council or damage the Council's reputation.
- ✘ Carrying out internet based searches on applicants or candidates for jobs in the Council, unless you are asked to by the candidate.
- ✘ Making a complaint about your employment publicly through the internet, intranet, media, or social media sites.

This list is not exhaustive.

ROLES AND RESPONSIBILITIES

The Council may be held legally liable for any statements made or contractual arrangements entered into by its employees through electronic means. It also has a responsibility to make sure the information we hold on clients, citizens and employees is held confidentially and securely. Therefore:-

1. All employees will be responsible for:

- making sure you have read and understood the ICT Acceptable Use Policy;
- meeting the standards of conduct set out in this Policy (see sections 4, 5 and 6) and any associated guidance which will be published on the intranet;
- undertaking any training as directed by your manager to make sure you understand how to use ICT systems correctly, including communication and use of language; and
- making sure that any Council ICT equipment that you take outside the work place including but not limited to laptops, mobile phones, iPads, are kept securely so that they cannot be used by others and are kept out of sight if unattended;
- reporting to your line manager any content, comment or information relating to the Council which you know or think could be illegal, defamatory, discriminatory or supports corruption or bribery;
- reporting to your line manager faulty equipment and the loss or theft of any equipment;
- reporting to your line manager actual or potential breaches of the Council's ICT security and/or loss of confidential data; and
- returning any Council ICT equipment to your manager when you leave the Council.

2. All managers will also be responsible for:

- making sure that your staff, including new recruits to the Council, are inducted in, aware of and understand the Policy and associated guidance and the consequences of any breach of the Policy;
- deciding which employees will have access to the Council's electronic equipment, data and information technology, to assist them in carrying out their duties and responsibilities, and to keep this under review;
- making sure that employees using ICT to carry out their duties have appropriate training in the use of the Council's ICT systems. This includes appropriate training on Data Protection and Information;

- taking action at the earliest signs of a breach of the Policy and /or Data Protection regulations;
- taking action when any breach or potential breach of security or confidentiality or loss or damage to ICT equipment is reported to you;
- authorising employees' use of personal electronic equipment and technology for work purposes when it is required to carry out their duties effectively;
- authorising employees' remote access to Councils networks and communications (e.g. e-mail/webmail) to allow occasional working from home;
- making sure that all personal information is processed in accordance with data protection legislation. [\[Insert link to data protection guidance on Orb\]](#)
- supporting the monitoring arrangements (see section 9) on the use of the Council's ICT systems; and
- making sure that employees are removed from the Council's ICT systems and any Council equipment is returned to the ICT solutions team when employees leave the Council.

3. The ICT Solutions Team is responsible for:

- defining the Council's ICT Strategy, approving ICT systems, equipment, networks and websites and making them available to staff to use during the course of their employment;
- approving any other systems which are not maintained by ICT Solutions, for use by staff (including e-mail systems), equipment (including personal phones or computers), networks or websites; and
- setting up, maintaining and managing a security configuration (set up) for Council ICT equipment.