POLICY TITLE

Information and Communications Technology (ICT) Acceptable Use Policy

REVISION DATE

The next revision is due November 2019 or sooner in case of change of legislation

REPLACES POLICY

This is the first policy.

POLICY NUMBER

POLICY AIM

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.

This policy applies to Skegness Town Council Employees and Councillors whether or not you are provided with or use Council ICT systems.

EXECUTIVE SUMMARY

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.

POLICY STATEMENT

1. DEFINITIONS OF ICT

1.1 Electronic equipment and technology includes all computer and telephone equipment including mobile phones, multimedia 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 or Councillor uses in the course of their employment. The Council's electronic equipment and technology will be referred to as "Council ICT systems."

1.2 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.

1.3 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.

1.4 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.

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

2.1 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 email and internet communications.

2.2 You must make sure that you communicate in a way that supports the Council's policies including those on equalities and that adheres to the principles of the Code of Conduct. 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, intimidates or stalks another person.

2.3 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.

2.4 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.

2.5 You must keep your password(s) confidential (don't share them with anyone else).

2.6 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.

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

3.1 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.

3.2 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 approval.

3.3 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 or Councillor Code of Conduct, Disciplinary Code or equality standards, must not be accessed from Council ICT Systems.

4. STANDARDS OF CONDUCT - USE OF SOCIAL MEDIA (see Social Media Policy)

4.1 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.

4.2 You must not use social media to harass, bully, stalk or behave in any other way that could damage your working relationships with staff, partners, members of the public or elected members.

IMPLEMENTATION

ROLES AND RESPONSIBILITIES

The Council may be held legally liable for any statements made or contractual arrangements entered into by its employees and Councillors 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:-

All employees and Councillors 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 2, 3 and 4) and any associated guidance which will be published on the intranet;
- 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 the Council 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 the Council any faulty equipment and the loss or theft of any equipment;

- reporting to the Council actual or potential breaches of the Council's ICT security and/or loss of confidential data; and

- returning any Council ICT equipment to the Council when you leave the Council.

If you use non Council issued equipment to access Council systems, these must only be "cloud based" applications where no data is stored or processed locally and the device is simply acting as a terminal. Should you download or process data or information locally on a non-Council device you will not be covered by the Council's Data Protection Registration and you may be breaking the law.

MONITORING

The Council may record the use of its systems to measure system security, performance, whether employees or Councillors are meeting the standards of conduct in this policy and for the prevention and detection of crime.

The Council may capture internet and e-mail activity, and reserves the right to access, retrieve and delete:

- all e-mail including in draft form, sent or received;

- all private and shared directories;

- all use of intra/internet and other communication techniques using the Council's ICT systems e.g. Twitter, blogs etc; and SharePoint sites

- all software and computer equipment.

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.

Under this policy both Employees and Councillors explicitly consent to the monitoring of communications and ICT use when using Council owned equipment or software.

Examples of Unacceptable Activity and Behaviour

Personal Behaviour

- Circulating non council 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.
- Sending, uploading, posting or publishing online any information or comment about an individual, company or organisation which is defamatory or libellous.

Security

- Sharing your password(s) or failing to comply with other security arrangements.
- 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 or your role as a Council Member– this is confidential to the Council.
- Giving information to the media if you are not authorised to do.
- Making public any information which may undermine confidence in the Council or damage the Council's reputation.

This list is not exhaustive.

POLICY CONSULTATION

The policy will be communicated to all Employees and Council Members.

POLICY APPROVAL

Council 4th November 2015

RELATED POLICIES & STRATEGIES

Information Security
Email and Internet
Data Protection