Croft Parish Council

Information and Communication Technology Policy

November 2025

Contents

1. What is Information and Communication Technology?

Information and Communication Technology (ICT) is a loose term which is used to describe a wide range of tools and techniques, usually electronic in nature, which speed up and/or aid communication.

Croft Parish Council recognises the importance of embracing ICT in order to ensure that its customers benefit from efficient levels of service delivery.

The Council supports the Government's aim of improving electronic access to public services.

2. Aims

The aims of this policy are to:

- Facilitate the ongoing development of the efficient management and delivery of the Council's services.
- Provide opportunities for staff to acquire and develop core ICT competencies; and
- Ensure that the Council's ICT systems are reviewed regularly and adjusted to meet new or changing needs.

3. Management

The Clerk has overall responsibility for ICT and the implementation of this Policy.

4. Technical Support

The Council shall appoint an independent and competent ICT support provider and will be subject to a 3-year review in order to confirm the service they provide and meet service delivery needs.

5. Security

a. Individuals shall:

- Be responsible for the Council's usernames and passwords.
- Protect user credentials against misuse;
- Not share or disseminate any user credentials with another person;
- Only attempt to access ICT where permissions have been given;
- Not misuse or alter the configuration or setting of any ICT;
- Not attempt to bypass or subvert ICT security controls;
- Not leave a computer system open if it is unattended;
- Operate a clear screen policy when you leaving ICT unattended, for example by temporary 'locking' the computer; and
- Protect all ICT portable media and devices at all times, in particular, when transporting them outside of Council premises, by security items within the fireproof storage within the Council Offices.

b. All ICT media and portable devices used to process Council information shall be password protected and encrypted.

c. Staff will seek to prevent inadvertent disclosure of personal or sensitive information by avoiding being overlooked when working.

d. Staff shall take care when printing information and carefully check the distribution list for any material to be transmitted.

e. Staff shall securely store or destroy any printed material which contains private information, sensitive, disclosive or identifiable records or which is not for public circulation.

f. Staff and elected Members shall not introduce unofficial software, hardware, removable media or files without appropriate authorisation.

g. Staff and elected Members shall report any security incident or suspected security incident to the Council as soon as is reasonably possible.

6. Hardware

The Council's computer systems and computer peripherals will be subject to annual review in order to confirm that they are meeting service delivery needs. All computer and computer peripherals will be listed and revisions/deletions will be assessed for replacement or upgrade over a maximum of a 3-year period.

7. Telephones and Related Systems

The Council does not have a dedicated telephone line.

8. Software

The Council's computer software will be subject to annual review in order to confirm that it is meeting service delivery needs and demand. In order to ensure adequate maintenance and development support, the Council shall normally avoid bespoke software packages.

The Council approved applications are:

Word Processing	Microsoft Word
Spreadsheets	Microsoft Excel
Presentations	Microsoft PowerPoint
Accounting	Microsoft Excel
Payroll	HMRC System

9. Internet Access

The Council recognises that the Internet is a valuable information resource with the potential to improve the delivery of its service. The Council will use the website provided by Lincolnshire County Council.

Access to the Internet must be approved by an authorised user - as appropriate, usually the Clerk.

Access to the Internet for 'leisure purposes' is permitted during authorised breaktimes.

Access for personal reasons is permitted in certain circumstances, however, it is the responsibility of the 'user' to ensure no illegal or prohibited sites are accessed; should this happen by error a report should be immediately submitted to the Clerk/Chair of the Council.

10. Email

The Council recognises that email is an increasingly popular, speedy and cost-effective method for communication and data transfer.

The Council requires that the Council Office, Franklin Hall, Halton Road, Spilsby has the capability of sending/receiving email messages and data.

Members of staff, elected members and authorised users shall ensure:

- Email use must be lawful and inoffensive - and be approved by an authorised user, normally the Clerk.
- They do not send personal or sensitive data over public networks such as the Internet unless an approved method of protection or encryption has been applied to it;
- They check that the recipients of e-mail messages are correct so that personal, or sensitive information is not accidentally released into the public domain;
- That personally owned email accounts are not used to conduct Council business;
- Personal use of the Internet shall be reasonable, proportionate and occasional and shall not interfere with the performance of your role or the performance of the system; and
- They do not use Council e-mail address(es) to send personal emails unless the item is marked as 'personal' and the sender clearly identifies that such communication.

11. Unacceptable Use

Members of Staff and authorised user shall ensure:

- Any security incident or suspected security incident is reported to the Council as soon as is reasonably possible.
- They do not send personal or sensitive data over public networks such as Internet unless an approved method of protection or encryption has been applied to it.
- They check that the recipients of e-mail messages are correct so that personal, or sensitive information is not accidentally released into the public domain;
- Personally owned e-mail accounts shall not be used to conduct Council business;
- They do not communicate information via an ICT system knowing it or suspecting it to be unacceptable within the context and purpose for which it is being communicated.
- They do not process or access racist, sexist, defamatory, offensive, illegal or otherwise inappropriate material;
- They do not carry out illegal, fraudulent or malicious activities;
- They do not store, process or display offensive or obscene material, such as pornography or hate literature;
- They do not annoy or harass another individual, for instance by sending chain letters, uninvited e-mail of a personal nature or by using lewd or offensive language; and
- They do not break copyright.

12. Personal Data

Any member of Staff processing personal data must comply with the eight enforceable principles of good practice (Data Protection Act 2018 and the General Data Protection Regulations 2018). These stipulate that data must be:

- Fairly and lawfully presented.
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the data subject's rights;
- Secure; and
- Not transferred to countries without adequate protection.

13. Data Protection

CONFIDENTIALITY

Passwords are to be used to restrict access to personal and/or confidential data. If there is any doubt about whether access to certain data should be restricted, guidance should be sought from the Council.

VIRUSES

All computers used to send/receive e-mails or to access the Internet must have recognised anti-virus software installed - such as Norton Anti-Virus or McAfee.

No disk, drive or memory stick from any external source shall be opened until it has been checked for viruses.

BACK-UPS

At the end of each working week, at least one back-up shall be taken of all current data files and stored in a fire proof container.

No data shall be stored in any internet storage areas (i.e., Cloud, Drive HQ, Drop Box, Spied Oak, Conclusions).

14. Training

The Council recognises that training Staff using new technology products is essential. Therefore:

- All users of IT Office Productivity facilities, such as word processing and spreadsheets, shall be given appropriate training.
- Adequate training in the use of specialised or bespoke software packages will be given to all users of that software; and
- Training will be given to users of any new software as part of the implementation programme.

15. Awareness

Individuals shall make themselves aware of, and comply with, requirements and legislation regarding information security and data protection along with any other legal, statutory or contractual obligations identified by the Council.

16. Monitoring

The Council reserves the right to monitor or record all communication systems including e-mail, electronic messaging and Internet use. Records of activity may be used by the Organisation for the following purposes:

- Quality Assurance.
- Conduct;
- Discipline;
- Performance; and
- Capability and/or criminal proceedings and any other purpose compliant with the regulatory and legislation framework in force and useful to support the Council's business.

17. Breaches of Policy

All Council employees have a contractual responsibility to be aware of and conform to the Council's values, rules, policies and procedures. Breaches of policy may lead to disciplinary proceedings.

Individuals who fail to comply with the Council's policies and who are not Council employees may have their access to Council information and ICT revoked and such action could have impacts on contracts with third party organisations.