

WELTON-BY-LINCOLN PARISH COUNCIL

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

1. What is Information and Communication Technology?

Information and Communication Technology (ICT) is 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.

Welton-by-Lincoln Parish Council recognises the importance of embracing ICT 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:

- i) facilitate the ongoing development of the efficient management and delivery of the Council's services.
- ii) provide opportunities for staff to acquire and develop core ICT competencies.
- iii) ensure that the Council's ICT systems are reviewed regularly and adjusted to meet new or changing need.

3. Management

The Parish 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 (currently SCIS (UK) Ltd, Lincoln) and will be subject to a 3-year review to confirm the service they provide meet service delivery needs.

5. Scope

This policy applies to all individuals who use Welton-by-Lincoln parish council's IT resources, including computers, networks, software, devices, data, and email accounts.

6. Security

a) Individuals shall:

- be responsible for the Parish 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 settings 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 leave ICT unattended, for example by temporary “locking” the computer.
 - protect all ICT portable media and devices at all times, in particular when transporting them outside of Council premises.
- 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)** Take care when printing information and by carefully checking 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.

7. Hardware

Computers and peripherals

The Parish Council's computer systems and computer peripherals will be subject to annual review to confirm that they are meeting service delivery needs.

All computers and computer peripherals will be listed, and revisions / deletions will be assessed for replacement or upgrade over a maximum of a 3-year period.

8. Telephones and related systems

Telephone/or answer machines (or such combined units, where supplied) will be maintained within the Parish Council office. Any information contained in outgoing messages (conveyed by the latter machine) will conform to national minimum standards with messages being clear and concise.

The Parish Clerk has the discretion to engage providers of more cost-effective telephone network services.

Except in exceptional circumstances, use of the telephone, related and electronic communication systems for personal use must be authorised by the Parish Clerk.

The Council's Facilities Team and Parish Office are issued with mobile phones. Mobile phones provided by Welton-by-Lincoln parish council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

All telephone and related systems will be assessed over a 3-year period and assessed for replacement/repair where necessary.

9. Audio-visual Equipment

The overhead projector equipment (stored at Manor Park) is and remains the property of Welton-by-Lincoln Parish Council. The service and repair of such equipment is the responsibility of Welton-by-Lincoln Parish Council.

10. Software

The Parish Council's computer software will be subject to annual review to confirm that it is meeting service delivery needs and demand.

The Parish Council approved applications are:

i)	word processing:	Microsoft Word
ii)	spreadsheets:	Microsoft Excel
iii)	accounting:	RBS (bespoke package)
iv)	payroll:	Basic PAYE tools HMRC payroll

Unauthorised installation of software on authorized devices, including personal software, is strictly prohibited due to security concerns.

11. Internet access

The Parish Council recognises that the Internet is a valuable information resource with the potential to improve the delivery of its services.

12. E-mail

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

The Council requires that the Parish Council Office has the capability of sending/receiving email messages and data.

Welton-by-Lincoln reserve the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

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

- i) e-mail use must be lawful and inoffensive - and be approved by an authorised user, normally the Parish Clerk.
- ii) 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.
- iii) 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.
- iv) that personally owned email accounts are not used to conduct Council business.
- v) 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.
- vi) they do not use Parish Council e-mail address(es) to send personal emails unless the item is marked as 'personal' and the sender clearly identifies that such communication.
- vii) Emails should be professional and respectful in tone.
- viii) Confidential or sensitive information must not be sent via email unless it is encrypted.
- ix) Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

13. Password and account security

Welton-by-Lincoln parish council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

14. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

15. Unacceptable Use

Members of staff, elected Members (Cllrs) and authorised users shall ensure:

- i) any security incident or suspected security incident to the Council as soon as is reasonably possible.
- ii) 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.
- iii) 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.
- iv) personally owned email accounts shall not be used to conduct Council business.
- v) 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.
- vi) they do not process or access racist, sexist, defamatory, offensive, illegal, or otherwise inappropriate material.
- vii) they do not carry out illegal, fraudulent, or malicious activities.
- viii) they do not store, process or displaying offensive or obscene material, such as pornography or hate literature.
- ix) 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.
- x) they do not break copyright.

16. Remote Access

The Parish Council recognises that staff may need to work from remote locations from time to time. To address this issue, provision for remote access is available. Log on and password information will be issued to staff members. Staff members shall report any security incident or suspected security incident to the Parish Clerk and the Council as soon as is reasonably possible.

17. Personal Data

Any member of staff processing personal data must comply with the eight enforceable principles of good practice (Data Protection Act 2018) and General Data Protection Regulations (GDPR) 2018.

These stipulate that data must be:

- a) fairly and lawfully processed.
- b) processed for limited purposes.
- c) adequate, relevant, and not excessive.
- d) accurate.

- e) not kept longer than necessary.
- f) processed in accordance with the data subject's rights.
- g) secure.
- h) not transferred to countries without adequate protection.

18. Data Protection

a) 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 Parish Clerk.

b) Viruses

All computers used to send/receive emails or to access the Internet must have recognised anti-virus software installed.

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

c) Back-ups

At the end of each working day, at least one back-up shall be taken of all current data files and taken off-site.

(Backed up in the cloud)

19. Training

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

- a) all users of IT office productivity facilities (such as word processing and spreadsheets) shall be given appropriate training.
- b) adequate training in the use of specialised or bespoke software packages will be given to all users of that software.
- c) training will be given to users of any new software as part of the implementation programme.

20. 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 Parish Council.

21. Monitoring

The Parish Council reserves the right to monitor or record all communication systems including email, electronic messaging, and internet use. Records of activity may be used by the organisation for the following purposes

- i) quality assurance
- ii) conduct
- iii) discipline
- iv) performance
- v) 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 activities.

22. 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.

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

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.

23. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

24. Contacts

For IT-related enquiries or assistance, users can contact the Parish Council Office and speak to the officer on duty.

All staff and councillors are responsible for the safety and security of Welton-by-Lincoln parish council's IT and email systems. By adhering to this IT and Email Policy, Welton-by-Lincoln parish council aims to create a secure and efficient IT environment that supports its mission and goals.

Policy adopted: 10th November 2025

Policy review: November 2026