COUNTESTHORPE PARISH COUNCIL

IT POLICY - Computer Use - Including the use of email/Internet

(also included in the Staff Handbook)

It is very important that the Council is able to keep its data secure. To assist with this, all employees are required to comply with instructions that may be issued from time to time regarding the use of Council-owned IT or communication systems.

Countesthorpe Parish Council IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

You should ensure that when leaving your workstation for any lengthy period, you lock your IT devices or log off if appropriate.

You must not attach any device to Council IT equipment without authorisation from the Parish Manager and you must not open attachments or click on links unless you know you can trust the source. Council portable IT devices must be kept secure and password protected at all times.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited for reasons of security concerns.

Your computer password is an important piece of confidential information and you should treat it that way. Do not share it with others, and make sure that it is not written down anywhere where an unauthorised person can find it.

Unauthorised access to any of the Council's IT and communication systems will amount to gross misconduct.

All sensitive and confidential Countesthorpe Parish Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

Countesthorpe 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.

Mobile devices provided by Countesthorpe Parish Council, such as laptops, should be secured with passcodes. When working remotely, users should follow the same security practices as if they were in the office.

No use of unauthorised data storage such as portable hard drives or memory sticks should be used without prior permission of the Parish Council Manager.

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 Parish Council Manager.

Internet Use

Employees with access to the internet on Council-owned IT devices should use that access responsibly.

Personal use during working hours will be treated as misconduct. From time to time the Council may block access to sites which it considers inappropriate but whether or not a specific site has been blocked, employees must not use the internet to view or download offensive or sexually explicit material. Any attempt to do so may, depending on the circumstances, amount to gross misconduct leading to dismissal.

Employees must not download any software, plugins or extensions on to Council-owned IT devices unless this is first cleared by an appropriate manager. Employees should also refrain from downloading music, video or any other entertainment content on any Council-owned IT device.

Firewalls and anti-virus software may be used to protect the Council's IT and communication systems. These must not be disabled or switched off without express permission from management.

Countesthorpe Parish Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

Email All email correspondence should be dealt with in the same professional and diligent manner as any other form of correspondence.If you have a Council email account you should be mindful of the fact that any email that you send will be identifiable as coming from the Council. You should therefore take care not to send anything via email that may reflect badly on the Council. In particular, you must not send content of a sexual, racist or discriminatory nature, junk mail, chain letters, cartoons or jokes from any email address associated with work.

Using a Council/work email address to send inappropriate material, including content of a sexual, racist or discriminatory nature, is strictly prohibited and may amount to gross misconduct. Should you receive any offensive or inappropriate content via email you should inform a member of management of this as soon as possible so that they can ensure that it is removed from the system.

You should also take care that emails will be seen only by the person intended. Particular care should be taken when sending confidential information that the email has been correctly addressed, marked 'private' / 'confidential' and not copied into those not authorised to see the information. Sending confidential information via email without proper authorisation or without taking sufficient care to ensure that it is properly protected will be treated as misconduct.

Countesthorpe Parish Council reserves 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.

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox. This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

SIGNED _____ (CHAIRMAN)

11th September 2025