Glanton Parish Council
Information Technology Policy

1. Purpose

This policy sets out the expectations for the appropriate and secure use of information technology, systems, devices and electronic communications used for council business.

The Council recognises the importance of protecting council information, personal data and digital systems from loss, misuse or unauthorised access.

2. Scope

This policy applies to councillors, employees, contractors and any authorised users who access council systems, devices, email accounts, cloud storage or other digital services.

It applies whether users are working from home, remotely, or from another location.

3. Council Systems and Equipment

Council systems and equipment are primarily provided for council business.

Reasonable personal use is permitted provided it:
- does not interfere with council business;
- does not create security risks;
- does not breach council policies or legislation.

All equipment should be treated with care and reasonable precautions should be taken to prevent loss, damage or unauthorised access.

Any faults, damage or loss involving council systems or data should be reported to the Clerk as soon as possible.

4. Passwords and Security

All accounts and devices used for council business must be protected with strong passwords.

The Council follows National Cyber Security Centre (NCSC) guidance recommending passwords made up of three random words.

Passwords must:
- not be shared;
- not be written down insecurely;
- be changed immediately if compromise is suspected.

Multi-factor authentication (MFA) should be enabled wherever possible.

Where password managers are used, they should be encrypted and reputable.

5. Personal Devices and Remote Working

The Council recognises that, due to its size and resources, some councillors and authorised users may use personal devices for council business.

Where personal devices are used:
• council business should be conducted through council email accounts where possible;
• devices must be password protected;
• secure WiFi connections should be used;
• council information should not be shared with unauthorised persons;
• council information should be deleted when no longer required;
• loss or theft of a device containing council information must be reported immediately.

Sensitive or confidential information should not be permanently stored on personal devices unless necessary.

6. Email and Electronic Communications

Council email accounts should be used for council business wherever possible.

Users must:
• communicate professionally and respectfully;
• take care when sending emails containing personal data;
• use BCC where appropriate for group emails;
• avoid forwarding confidential information inappropriately;
• not open suspicious links or attachments.

Emails may form part of the council's official records and may be subject to disclosure under relevant legislation.

7. Internet and Software Use

Users must not knowingly:
• access inappropriate, offensive or unlawful material using council systems;
• download unauthorised software;
• breach copyright restrictions;
• use council systems for unlawful activity.

Care should be taken when downloading files or using external websites to reduce cyber security risks.

8. Social Media

Councillors, staff and authorised users should act professionally when using social media in relation to council matters.

Users must not:
• disclose confidential information;
• publish personal data unlawfully;
• imply they are speaking on behalf of the Council unless authorised;
• post material likely to damage the reputation of the Council.

Councillors should remain mindful of the Members' Code of Conduct and Nolan Principles when using social media.

9. Data Protection and Data Breaches

Use of council systems must comply with the Council's Data Protection and Privacy Policy.

Any actual or suspected data breach, cyber incident or loss of council information must be reported to the Clerk immediately.

10. Monitoring

The Council reserves the right to investigate misuse of its systems, accounts or information where necessary and proportionate.

Due to the Council's size and resources, routine active monitoring of users is not normally carried out.

11. Review

This policy will be reviewed every two years or sooner if required by changes to legislation, guidance or council operations.