Gosfield Parish Council
IT & Cyber Security Policy

1. Policy Statement

The Parish Council recognises the importance of maintaining secure and reliable information technology systems and protecting the confidentiality, integrity, and availability of the information it holds.

This policy establishes the standards and responsibilities for the use, management, and protection of the Council's information assets, systems, devices, and data. It supports compliance with relevant legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Freedom of Information Act 2000, and other applicable legal and regulatory requirements.

---

2. Purpose

The purpose of this policy is to:

- Protect Council information and IT systems from unauthorised access, loss, damage, theft, or misuse.
- Reduce the risk of cyber incidents and data breaches.
- Define acceptable use of Council technology resources.
- Establish responsibilities for information security.
- Support business continuity and service delivery.

---

3. Scope

This policy applies to:

- Parish Councillors
- The Parish Clerk
- Employees
- Contractors
- Volunteers
- Any individual granted access to Council systems, devices, networks, or information

The policy applies to:

- Council-owned computers and devices
- Personal devices used for Council business
- Email systems
- Cloud storage services
- Websites and social media accounts
- Digital records and information assets

---

4. Roles and Responsibilities

Parish Council

The Council shall:

- Approve and periodically review this policy.
- Ensure appropriate resources are available for cyber security.
- Support compliance with legal obligations.

Parish Clerk

The Clerk shall:

- Act as the primary administrator of Council IT systems.
- Ensure implementation of this policy.
- Maintain records of IT assets and user accounts.
- Coordinate responses to security incidents.
- Ensure appropriate backups are maintained.

Councillors, Staff and Users

All users shall:

- Follow this policy.
- Protect Council information.
- Report security incidents immediately.
- Complete any required cyber security awareness training.

---

5. Acceptable Use

Council IT systems are provided primarily for Council business.

Users must:

- Use systems responsibly and professionally.
- Access only information required for their role.
- Protect confidential and personal information.
- Follow security procedures and guidance.

Users must not:

- Share passwords.
- Access inappropriate, offensive, or illegal content.
- Circumvent security controls.
- Install unauthorised software.
- Use Council systems for personal commercial purposes.

Limited personal use may be permitted provided it:

- Does not interfere with Council business.
- Does not incur additional costs.
- Complies with this policy.

---

6. Password Management

All users must:

- Use strong passwords consisting of at least 12 characters.
- Use a unique password for each Council account.
- Avoid using easily guessed information.
- Keep passwords confidential.

Passwords must never be:

- Shared with others.
- Written in publicly accessible locations.
- Sent via email or unsecured messages.

Multi-factor authentication (MFA) must be enabled wherever available, particularly for:

- Email accounts
- Cloud storage services
- Banking and finance systems
- Website administration accounts

---

7. Email Security

Council email accounts should be used for official Council business whenever possible.

Users must:

- Verify the legitimacy of unexpected emails.
- Avoid opening suspicious attachments or links.
- Report phishing attempts immediately.

Users must not:

- Forward chain emails.
- Send confidential information without appropriate safeguards.
- Use personal email accounts for sensitive Council business unless approved.

---

8. Device Security

Council-owned devices must:

- Be password protected.
- Use automatic screen locking.
- Have current operating system updates installed.
- Use reputable anti-malware protection where appropriate.

Users must:

- Keep devices physically secure.
- Avoid leaving devices unattended in public locations.
- Report lost or stolen devices immediately.

---

9. Personal Devices (BYOD)

Where personal devices are used for Council business:

- The device must be protected by a password or biometric security.
- Software updates must be installed promptly.
- Council information must be stored securely.
- Council data must be deleted when no longer required.

The Council reserves the right to require Council information to be removed from personal devices when appropriate.

---

10. Data Protection and Information Handling

All personal data must be processed in accordance with:

- UK GDPR
- Data Protection Act 2018
- Council Data Protection Policies

Users must:

- Access only information necessary for their duties.
- Store personal information securely.
- Dispose of information securely when no longer needed.

Personal data should not be retained longer than required under the Council's retention schedule.

---

11. Cloud Services and Storage

Council information stored electronically should be held within approved systems.

Where cloud services are used:

- Appropriate access controls must be implemented.
- MFA should be enabled.
- Data sharing permissions should be reviewed regularly.
- Only authorised users should have access.

---

12. Website and Social Media Security

The Council's website and social media accounts must be protected by:

- Strong passwords.
- MFA where available.
- Restricted administrator access.

Access should be reviewed regularly and removed promptly when no longer required.

Official communications should only be published by authorised individuals.

---

13. Software Management

Only authorised software should be installed on Council devices.

Software must:

- Be legally licensed.
- Be supported and regularly updated.
- Be removed when no longer required.

Users must not download or install software without approval from the Clerk or designated administrator.

---

14. Backup and Recovery

The Council shall maintain appropriate backups of critical information.

Backups should:

- Be performed regularly.
- Be stored securely.
- Be protected from unauthorised access.
- Be periodically tested to ensure recovery is possible.

Critical records should be recoverable following system failure, cyber attack, or accidental deletion.

---

15. Cyber Security Awareness

Users should remain vigilant against cyber threats including:

- Phishing emails
- Social engineering

- Malware
- Ransomware
- Fraudulent payment requests

The Council should encourage periodic cyber security awareness training and guidance.

---

16. Incident Reporting

Any actual or suspected security incident must be reported immediately to the Parish Clerk.

Examples include:

- Phishing attacks
- Malware infections
- Lost or stolen devices
- Unauthorised access
- Accidental disclosure of information
- Data breaches

The Clerk shall:

- Record incidents.
- Assess risks.
- Take appropriate corrective action.
- Escalate data breaches where required under applicable legislation.

---

17. Business Continuity

The Council shall seek to maintain continuity of operations in the event of:

- Cyber attacks
- Equipment failures
- Loss of internet connectivity
- Data corruption
- Natural disasters

Appropriate recovery arrangements should be reviewed periodically.

---

18. Monitoring and Compliance

The Council reserves the right, where lawful and proportionate, to:

- Monitor use of Council IT systems.
- Audit compliance with this policy.
- Investigate suspected misuse.

Failure to comply with this policy may result in:

- Removal of system access.
- Disciplinary action where applicable.
- Referral to law enforcement where appropriate.

---

19. Related Policies

This policy should be read alongside:

- Data Protection Policy
- Privacy Notice
- Freedom of Information Publication Scheme
- Records Retention Policy
- Social Media Policy
- Financial Regulations
- Standing Orders

---

20. Policy Review

This policy shall be reviewed:

- Annually; or
- Following a significant cyber security incident; or
- Following major changes in legislation, technology, or Council operations.

Adopted
Date 22nd June 2026
Minute reference 26/122 Item 4
Signed ……
Review Date: May 2027