PEASMARSH PARISH COUNCIL

Parish Council IT & Cyber Security Policy

The IT & Cyber Security Policy adopted by Peasmarsh Parish Council in March 2026 is set out below. This policy is reviewed every two years or in response to significant legislative or operational changes.

Contents

Introduction

This IT & Cyber Security Policy sets out how the Parish Council manages information technology, digital systems, and data securely and responsibly. It is proportionate to a oneclerk parish council and is designed to:

1.1. Protect the confidentiality, integrity, and availability of council information
1.2. Reduce the risk of cyber incidents, fraud, and data loss
1.3. Support compliance with:
    1.3.1. The Accounts and Audit Regulations 2015
    1.3.2. UK GDPR and the Data Protection Act 2018
    1.3.3. The Transparency Code for Smaller Authorities
    1.3.4. AGAR Assertion 10 – appropriate arrangements for cyber security

Scope

2. This policy applies to:
    2.1. All Parish Councillors
    2.2. The Clerk / Responsible Financial Officer (RFO)
3. It covers all IT systems used for council business, whether council-owned or clerk-owned, including:
    3.1. Computers, laptops, tablets, and mobile phones
    3.2. Email accounts and cloud storage
    3.3. Financial systems and online banking
    3.4. The council website and social media
    3.5. Electronic records and backups

Roles and Responsibilities (One-Officer Council)

4. **Parish Council –** The Parish Council is collectively responsible for:
    4.1. Approving and reviewing this policy
    4.2. Ensuring cyber security is included in the risk register
    4.3. Receiving reports of incidents and assurance from the Clerk
    4.4. Providing appropriate resources within its budget
5. **Clerk / RFO –** As the sole officer of the Council the Proper Officer/RFO is responsible for:
    5.1. Day-to-day operation of council IT systems
    5.2. Implementing this policy in practice
    5.3. Maintaining a simple inventory of:
        5.3.1. Devices used for council business
        5.3.2. Key accounts (email, banking, website, cloud storage)
    5.4. Ensuring backups are taken and tested
    5.5. Reporting cyber incidents to the Chair and Council
6. To maintain separation of duties, councillors will provide oversight rather than operational control, for example through review of bank reconciliations and risk assessments.

Risk Management (Aligned to Risk Register)

7. The council recognises cyber security as a corporate risk.

8. Cyber risks recorded in the risk register include:

- **8.1.** Loss or theft of clerk device
- **8.2.** Phishing or email fraud
- **8.3.** Online banking fraud
- **8.4.** Data loss or corruption
- **8.5.** Website compromise

9. Controls linked to the risk register include:

- **9.1.** Strong passwords and two-factor authentication
- **9.2.** Regular data backups
- **9.3.** Independent verification of financial instructions
- **9.4.** Antivirus, updates, and device security
- **9.5.** Councillor oversight and review

10. The risk register will be reviewed at least annually and whenever there is a significant change to IT arrangements.

Acceptable Use of IT and Artificial Intelligence (AI)

11. IT systems used for council business must only be used for legitimate council purposes.

12. Where clerk-owned devices are used, council data must be:

- **12.1.** Kept separate where practicable
- **12.2.** Protected by passwords and encryption

13. Council data must not be shared or stored insecurely.

14. No unauthorised software, online services, or AI tools may be used for council business.

Use of Artificial Intelligence (AI)

15. The Parish Council recognises that Artificial Intelligence (AI) tools (such as text-generation, summarisation, transcription, or data analysis tools) may be used to support administrative efficiency. Their use must be proportionate, transparent, and controlled.

- **15.1.** AI tools may only be used for supporting tasks, such as:
  - **15.1.1.** Drafting documents or correspondence
  - **15.1.2.** Summarising non-confidential information
  - **15.1.3.** Improving clarity and consistency of text
- **15.2.** AI tools must **not** be used for:
  - **15.2.1.** Automated decision-making
  - **15.2.2.** Processing or inputting sensitive personal data
  - **15.2.3.** Making financial decisions or authorising payments

15.2.4. Producing final outputs without human review

Data Protection and AI

16. No personal data, confidential information, or financial details may be entered into public or consumer AI systems.

17. Any output generated using AI must be reviewed, checked for accuracy, and approved by the Clerk before use.

18. The Clerk remains fully responsible for the accuracy, legality, and appropriateness of all council documents, whether or not AI tools were used in their preparation.

Access Control and Passwords

19. Access to council systems is limited to the Clerk and authorised councillors only

20. Strong passwords must be used:

- **20.1.** Minimum 12 characters
- **20.2.** Not reused across personal accounts

21. Two-factor authentication (2FA) must be enabled where available, particularly for:

- **21.1.** Email
- **21.2.** Online banking
- **21.3.** Cloud storage
- **21.4.** Website administration

22. Passwords must only be written down in password locked documents and not be written down or shared. The Chairman will be given the password for the password document in a sealed envelope.

Email and Phishing Controls

23. Council business should be conducted using a council-controlled email account where possible. Personal emails should not be used for Council business.

24. The Clerk and councillors must remain alert to phishing and impersonation attempts. Any potential issues must be reported to the Proper Officer who will pass on the matter to the IT provider (currently Netwise).

25. Requests for payments or changes to bank details must:

- **25.1.** Never rely solely on email unless sent directly by the Proper Officer to notify payments set up on the bank account.
- **25.2.** Any other request must be independently verified and confirmed by the Proper Officer.

Data Protection

26. Personal data will be processed in accordance with the council's Data Protection Policy.

27. Only data necessary for council business will be retained.

28. Data will be stored securely and deleted when no longer required.

29. Data breaches will be managed in line with ICO guidance.

Backups and Business Continuity

30. All critical council data will be backed up regularly

31. Backups will be:

- **31.1.** Automatic where possible managed through the IT provider (currently Netwise).
- **31.2.** Stored securely, currently this is done via the cloud and encrypted external storage.
- **31.3.** Backups will be tested periodically via the IT provider (currently Netwise).
- **31.4.** The council will maintain arrangements to continue essential functions if IT systems fail.

Devices and Software

32. Devices used for council business must:

- **32.1.** Be password protected.
- **32.2.** Automatically lock when unattended.
- **32.3.** Operating systems and applications must be kept up to date.
- **32.4.** Antivirus and firewall protection must be enabled.

Website and Online Services

33. The council website will be managed securely

34. Administrator access will be restricted

35. Strong passwords and 2FA will be used where available

36. The website will comply with transparency and accessibility requirements

Financial Systems and Online Banking

37. Online banking access will be restricted to authorised users

38. Dual authorisation will be used wherever the bank allows

39. Changes to bank details will be independently verified

40. Bank reconciliations will be reviewed by councillors

Cyber Incident Procedure (Appendix A)

41. A cyber incident is any event that compromises, or has the potential to compromise, the confidentiality, integrity, or availability of the Parish Council's information, IT systems, or online services.

42. Given the council's reliance on electronic systems for administration, finance, and communication, even a minor incident (such as a suspected phishing email or temporary loss of access to an account) can present a risk.

43. This procedure ensures that incidents are handled promptly, consistently, and proportionately, with clear accountability, to minimise harm, prevent escalation, and demonstrate effective governance and compliance with data protection and audit requirements. Please see Appendix A for the full procedure.

Training and Awareness

44. The Clerk and councillors will maintain basic cyber security awareness

45. This policy will be included in councillor induction

Review and Approval

46. This policy will be reviewed annually and following any cyber incident.

47. The council confirms that this policy supports compliance with AGAR Assertion 10.

Appendix A – Cyber Incident Procedure

What is a Cyber Incident?

- Loss or theft of a device
- Phishing or suspected fraud
- Unauthorised system access
- Data loss or disclosure

Immediate Actions

- Disconnect affected device or account if safe to do so
- Change passwords immediately
- Inform the Chair of the Council

Follow-Up Actions

- Record the incident and actions taken
- Assess whether personal data is involved
- Report to the ICO within 72 hours if required
- Review controls and update the risk register

Appendix B – AGAR Assertion 10 Evidence Checklist

Policy & Governance

- IT & Cyber Security Policy adopted and minuted
- Policy reviewed within last 12 months

Risk Management

- Cyber risks included in risk register
- Controls documented and reviewed

Access & Security

- Strong passwords in use
- Two-factor authentication enabled where available
- Devices password protected and updated

Backups

- Regular backups in place
- Backups tested

Financial Controls

- Dual authorisation for payments (where possible)
- Independent verification of bank detail changes

Training & Awareness

- Clerk and councillors aware of cyber risks

Incident Management

- Cyber Incident Procedure in place
- No unreported incidents (or incidents documented)