

BADGERS MOUNT PARISH COUNCIL -INFORMATION TECHNOLOGY (IT) POLICY

Document Control Version 2.0

Policy Owner	Parish Clerk
Approved by	Badgers Mount Parish Council
Adoption Date	[To be completed]
Review Date	Annually from adoption
Next Review	[To be completed]

Contents

1. Purpose
2. Scope
3. Guiding Principles
4. The Council's IT Environment
5. Roles and Responsibilities
6. Council Equipment
7. Bring Your Own Device (BYOD)
8. Council Email and Electronic Communications
9. Passwords and Authentication
10. Cloud Storage and Document Management
11. Information Security
12. Cyber Security
13. Artificial Intelligence (AI)
14. Remote Working
15. Business Continuity
16. Data Protection and Confidentiality
17. Freedom of Information and Records Management
18. Social Media
19. Incident Reporting
20. Training and Awareness
21. Procurement of IT Hardware and Software
22. Monitoring and Compliance
23. Breaches of this Policy
24. Policy Review

Appendices

- A. Password Standard
- B. Device Security Checklist
- C. Cyber Incident Response Checklist
- D. Acceptable Use Summary

1. Purpose

Badgers Mount Parish Council recognises that digital technology is fundamental to the efficient delivery of modern local government. Information held electronically is one of the Council's most valuable assets and must be protected from loss, unauthorised access, accidental disclosure and cyber attack.

This policy establishes the principles governing the secure, lawful and responsible use of information technology by the Council. It aims to:

- protect the confidentiality, integrity and availability of Council information;
- support compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other relevant legislation;
- promote good cyber security practices;
- provide clear guidance for Councillors and the Clerk when using digital technology;
- safeguard public confidence in the Council's handling of information;
- ensure business continuity through secure storage and appropriate management of electronic records.

The Council recognises that, as a small parish council, its technology arrangements differ significantly from those of larger principal authorities. Accordingly, this policy has been designed to be proportionate, practical and appropriate to the Council's size, resources and operational requirements whilst maintaining high standards of governance and information security.

2. Scope

This policy applies to:

- all elected Councillors;
- the Parish Clerk;
- any person authorised to access Council information, systems or electronic records on behalf of the Council.

The policy applies regardless of where Council business is undertaken, including:

- home working;
- Council meetings;
- site visits;
- remote access;
- mobile working.

It applies to all Council information regardless of whether it is:

- electronic;
- paper based;
- stored locally;
- stored in cloud services;
- transmitted by email or other approved electronic means.

3. Guiding Principles

The Council's approach to information technology is based upon the following principles.

3.1 Proportionality

Technology arrangements shall be proportionate to the size and resources of the Council.

The Council will implement security measures appropriate to the risks it faces without creating unnecessary complexity.

3.2 Security

Council information shall be protected against:

- unauthorised access;
- accidental loss;
- corruption;
- cyber attack;
- misuse.

3.3 Accountability

Every person handling Council information is responsible for protecting it.

Information security is not solely the responsibility of the Clerk.

Councillors share responsibility for safeguarding the Council's information assets.

3.4 Legal Compliance

The Council will comply with all relevant legislation including:

- UK GDPR;
- Data Protection Act 2018;

- Freedom of Information Act 2000;
- Environmental Information Regulations 2004;
- Copyright, Designs and Patents Act 1988;
- Local Government Act 1972;
- relevant guidance issued by the Information Commissioner's Office (ICO);
- Relevant cyber security guidance published by the National Cyber Security Centre (NCSC).

3.5 Good Governance

Digital systems shall support transparency, accountability, efficient administration and effective decision making.

4. The Council's IT Environment

Badgers Mount Parish Council is a small parish council comprising five elected Councillors and one Parish Clerk.

Unlike larger councils, Badgers Mount Parish Council does not maintain dedicated offices, servers or an internal IT department.

The Council's technology arrangements are intentionally simple and proportionate.

Current arrangements include:

- one Council-owned laptop issued exclusively to the Parish Clerk;
- one Council-owned mobile telephone issued exclusively to the Parish Clerk;
- individual **.gov.uk** email accounts for every Councillor and the Clerk;
- secure cloud-based storage for official Council documents;
- secure electronic backups of Council records;
- Councillors using their own personal devices when carrying out Council duties;
- electronic records maintained and administered by the Clerk as the Council's Proper Officer.

The Clerk is the custodian of the Council's official electronic records.

Official documents shall normally be stored within the Council's approved cloud storage environment and, where appropriate, on the Council laptop.

The Council does not maintain local servers or permanently store official records on Councillors' personal devices.

5. Roles and Responsibilities

5.1 The Council

The Council is responsible for:

- approving this policy;
- ensuring sufficient resources are available to maintain appropriate cyber security;
- promoting a culture of good information governance;
- reviewing this policy periodically.

5.2 The Parish Clerk

As Proper Officer of the Council, the Clerk has day-to-day responsibility for the administration of the Council's information technology arrangements.

This includes:

- maintaining the Council's official electronic records;
- administering document storage;
- managing Council-owned equipment;
- ensuring software updates are applied promptly;
- maintaining appropriate anti-malware protection;
- managing user access to Council systems;
- reporting significant cyber security risks to the Council;
- coordinating responses to any information security incidents;
- ensuring compliance with this policy.

5.3 Councillors

Councillors are responsible for:

- protecting Council information held on their personal devices;
- using their Council **.gov.uk** email account for official Council business;
- maintaining appropriate password security;
- complying with this policy;
- reporting suspected cyber incidents promptly;
- protecting confidential information at all times.

Councillors must recognise that information received in their role as elected members may be subject to legal disclosure, Freedom of Information legislation or data protection requirements.

5.4 Shared Responsibility

Every individual who accesses Council information has a personal responsibility to:

- act responsibly;
- remain vigilant to cyber threats;
- protect confidential information;
- follow this policy;
- report concerns without delay.

Information security is everyone's responsibility.

6. Council Equipment

6.1 Council-Owned Equipment

Badgers Mount Parish Council currently owns:

- one laptop issued exclusively to the Parish Clerk; and
- one mobile telephone issued exclusively to the Parish Clerk.

These devices are provided solely for carrying out official Council business and remain the property of the Council.

The Clerk is responsible for ensuring that Council-owned equipment is:

- maintained in good working order;
- protected by strong passwords and Multi-Factor Authentication (MFA) where available;
- configured to install security updates promptly;
- protected by reputable anti-malware software;
- stored securely when not in use.

Council equipment must not be loaned to family members or other third parties.

6.2 Care of Equipment

Users must take reasonable care of Council equipment by:

- preventing accidental damage;
- avoiding exposure to excessive heat, moisture or physical impact;
- not leaving equipment unattended in public places;
- securing equipment when travelling.



Where equipment is left temporarily in a vehicle, it should be concealed from view and only where absolutely unavoidable.

6.3 Software Installation

Only software that is necessary for Council business should be installed on Council-owned devices.

Software should only be obtained from reputable sources and appropriately licensed.

Unauthorised software must not be installed.

Where there is uncertainty, approval should be sought from the Clerk before installation.

7. Bring Your Own Device (BYOD)

7.1 Council Approach

Badgers Mount Parish Council recognises that, as a small parish council, it is neither practical nor proportionate to issue computing equipment to every Councillor.

Accordingly, Councillors are permitted to use their own computers, tablets and mobile phones when undertaking Council duties.

This arrangement is commonly known as **Bring Your Own Device (BYOD)**.

The Council considers BYOD to be appropriate provided suitable safeguards are maintained.

7.2 Minimum Security Requirements

Any personal device used to access Council information should:

- be protected by a strong password, PIN or biometric authentication;
- be configured to lock automatically after a period of inactivity;
- have current operating system updates installed;
- have anti-malware protection where appropriate;
- connect through secure internet connections;
- be capable of being remotely located or erased where the technology permits.

7.3 Storage of Council Information

Councillors should avoid permanently storing Council documents on personal devices wherever practicable.

The Council's approved cloud storage is the primary location for official electronic records.

Where documents are temporarily downloaded for meetings or offline working they should be deleted when no longer required.

Personal data should never be retained unnecessarily on personal devices.

7.4 Loss of Personal Devices

If a personal device containing Council information is lost, stolen or compromised, the user must notify the Clerk immediately.

The Clerk will assess whether:

- Council information has been compromised;
- passwords require changing;
- access permissions should be revoked;
- the incident constitutes a personal data breach requiring further action.

Prompt reporting enables the Council to minimise potential harm.

8. Council Email and Electronic Communications

8.1 Official Email Accounts

Every Councillor and the Parish Clerk is provided with an individual **.gov.uk** email address.

Official Council business should normally be conducted using these accounts.

Using Council email ensures:

- greater security;
- continuity of Council records;
- compliance with Freedom of Information legislation;
- easier records management;
- professional communication with residents and partner organisations.
-

8.2 Personal Email Accounts

Personal email accounts should not normally be used for Council business.

Where exceptional circumstances make this unavoidable, any Council correspondence should be forwarded promptly to the relevant Council email account so that an official record is retained.

8.3 Email Etiquette

Users should:

- communicate courteously and professionally;
- avoid unnecessary "Reply All" responses;
- check recipients carefully before sending;
- ensure attachments are appropriate;
- consider whether a telephone call would be more effective than lengthy email exchanges.

8.4 Confidential Information

Before sending confidential or sensitive information electronically, users should consider:

- whether email is the most appropriate communication method;
- whether all recipients are authorised to receive the information;
- whether additional protection (such as password-protected attachments) is appropriate.

Particular care should be taken when sending documents containing personal information.

8.5 Suspicious Emails

Users should remain alert to phishing attempts.

Emails should be treated with caution where they:

- request passwords;
- request urgent financial action;
- contain unexpected attachments;
- contain unfamiliar links;
- originate from unknown or suspicious senders.

If in doubt, users should not click links or open attachments and should contact the sender by an alternative method before responding.

9. Passwords and Authentication

9.1 General Principles

Passwords are the first line of defence against unauthorised access.

Every user is responsible for maintaining secure authentication credentials.

9.2 Password Standard

The Council adopts the National Cyber Security Centre recommendation of using **three random words** to create memorable but strong passwords.

Examples include combinations of unrelated words rather than predictable phrases.

Passwords should:

- be unique for each system;
- not be reused across multiple services;
- not contain easily guessed personal information.

9.3 Password Sharing

Passwords are personal.

Users must not:

- share passwords;
- disclose passwords by email;
- write passwords where they may be seen by others.

Where emergency access arrangements are required, these shall be managed by the Clerk in a secure manner.

9.4 Multi-Factor Authentication (MFA)

Multi-Factor Authentication significantly reduces the likelihood of unauthorised access.

MFA shall be enabled wherever it is available, particularly for:

- Council email accounts;
- cloud storage;
- Microsoft 365 services;

- financial systems;
- website administration.

9.5 Password Changes

Passwords should be changed immediately where:

- compromise is suspected;
- phishing has occurred;
- a device has been lost or stolen;
- instructed following a cyber security incident.

Routine scheduled password changes are not required unless circumstances indicate increased risk, reflecting current National Cyber Security Centre guidance.

10. Cloud Storage and Document Management

10.1 Official Records

The Parish Clerk is responsible for maintaining the Council's official electronic records.

The Council's approved cloud storage is the authoritative location for Council documents.

Where duplicate copies exist, the version held within the approved cloud storage shall normally be regarded as the official record.

10.2 Document Management

Council documents should be organised using consistent naming conventions and folder structures to ensure they remain accessible and easily identifiable.

Where possible:

- only one working version of a document should exist;
- superseded drafts should be removed or archived appropriately;
- final approved documents should be clearly identified.

10.3 Access Permissions

Access to electronic documents should be limited to those requiring access for legitimate Council business.

Permissions should be reviewed periodically by the Clerk.

10.4 Backups

The Council recognises the importance of protecting electronic information against accidental loss.

Official records should be retained within systems that provide secure backup and recovery arrangements.

The Clerk should periodically satisfy themselves that backup arrangements remain effective.

10.5 Retention and Disposal

Electronic records shall be retained in accordance with the Council's Records Retention Policy.

When records reach the end of their retention period they shall be securely deleted or archived as appropriate.

Personal information shall not be retained longer than necessary.

11. Information Security

11.1 General Principles

Information is one of the Council's most valuable assets and must be protected throughout its lifecycle.

The Council is committed to ensuring that information is:

- **Confidential** – accessible only to those authorised to see it;
- **Accurate** – complete, reliable and protected from unauthorised alteration;
- **Available** – accessible to authorised users when required.

All Councillors and the Clerk share responsibility for protecting Council information, whether held electronically or in paper form.

11.2 Classification of Information

Council information should be handled according to its sensitivity.

Public Information

Information intended for publication, including:

- agendas;
- approved minutes;
- adopted policies;
- information published under the Publication Scheme.

This information may be freely shared.

Internal Information

Routine working documents intended for Council business but not yet published.

Examples include:

- draft reports;
- working papers;
- internal correspondence.

These should only be shared with authorised recipients.

Confidential Information

Information requiring a higher level of protection, including:

- personal data;
- staffing matters;
- commercially sensitive information;
- legally privileged advice;
- confidential tender information;
- information discussed in confidential Council sessions.

Such information must only be accessed by those authorised to do so.

11.3 Physical Security

Users should ensure that:

- devices are locked when left unattended;
- confidential papers are not left visible;
- conversations involving confidential information cannot be overheard;
- screens containing confidential information cannot easily be viewed by others.

Reasonable precautions should always be taken when working outside the home.

11.4 Printing

Printing should be kept to the minimum necessary.

Where confidential documents are printed they should:

- be collected immediately;
- stored securely;
- shredded when no longer required.

11.5 Portable Storage Devices

The use of USB memory sticks or other removable storage devices should be avoided wherever practical.

Where their use is unavoidable:

- only encrypted devices should be used;
- files should be transferred to the Council's approved cloud storage as soon as practicable;
- removable media should not be used as permanent storage.

12. Cyber Security

12.1 Commitment

The Council recognises that cyber threats continue to evolve and represent one of the greatest risks to local authorities of every size.

Although Badgers Mount Parish Council is a small authority, it holds valuable information and therefore adopts a proactive approach to cyber security.

The Council aims to follow the principles of the National Cyber Security Centre's **Cyber Essentials** scheme wherever practical.

12.2 Security Measures

The Council will maintain appropriate safeguards including, where applicable:

- strong passwords;

- Multi-Factor Authentication;
- reputable anti-malware software;
- operating system updates;
- application security updates;
- secure cloud storage;
- secure backups.

12.3 Software Updates

Security updates should be installed promptly.

Users should not postpone updates unnecessarily.

Outdated software represents a significant cyber security risk.

12.4 Phishing

Phishing emails are the most common form of cyber attack affecting local councils.

Users should be particularly cautious where messages:

- create urgency;
- request passwords;
- request payment;
- ask for bank details;
- request gift cards or vouchers;
- contain unexpected attachments;
- contain unfamiliar internet links.

Where there is doubt, users should verify requests using a different communication method before taking action.

12.5 Financial Fraud

Particular care should be taken where emails request changes to:

- supplier bank details;
- payment instructions;
- invoices;
- grant payments.

No changes to banking arrangements should be made solely on the basis of an email.

Independent verification should always be obtained.

12.6 Cyber Incidents

Examples of cyber incidents include:

- malware infection;
- ransomware;
- successful phishing attack;
- unauthorised system access;
- lost devices;
- compromised passwords;
- accidental disclosure of personal information.

Any suspected incident must be reported immediately to the Clerk.

Where the Clerk is affected, the Chairman should be informed without delay.

13. Responsible Use of Artificial Intelligence (AI)

13.1 Purpose

The Council recognises that Artificial Intelligence (AI) tools are becoming increasingly common and can assist in improving efficiency and productivity.

AI may be used to support administrative work, provided it is used responsibly and does not compromise confidentiality, accuracy or legal compliance.

13.2 Appropriate Uses

AI may be used to assist with tasks such as:

- improving grammar and readability;
- summarising lengthy documents;
- producing first drafts of reports;
- generating ideas;
- formatting documents;
- preparing communication drafts.

AI should be regarded as an **assistant**, not a decision-maker.

13.3 Human Oversight

All AI-generated material must be reviewed by the Clerk or an authorised Councillor before it is:

- published;
- presented to Council;
- issued to residents;
- relied upon for decision-making.

Users remain responsible for the accuracy of all content.

13.4 Protection of Confidential Information

Users must not enter confidential or personal information into publicly available AI systems unless the Council has approved the service and appropriate contractual and data protection safeguards are in place.

Examples include:

- names of residents;
- personal addresses;
- financial information;
- staffing matters;
- confidential reports;
- legal advice.

Where possible, prompts should be anonymised.

13.5 Decision Making

AI must never:

- make decisions on behalf of the Council;
- replace professional judgement;
- determine statutory decisions;
- be relied upon without verification.

Responsibility for all decisions remains with the Council and its Proper Officer.

13.6 Internet Use

Internet access should be used responsibly and primarily for legitimate Council purposes.

Users should not knowingly:

- access unlawful material;
- download pirated software;
- visit malicious websites;
- install unauthorised applications;
- deliberately bypass security controls.

Copyright legislation must always be respected.

Information obtained from the internet should be assessed critically, recognising that online content is not always accurate or reliable.

14. Remote Working

The Council recognises that both the Clerk and Councillors routinely undertake Council business from home or other remote locations.

When working remotely, users should:

- use secure Wi-Fi connections wherever possible;
- avoid conducting confidential work over unsecured public Wi-Fi;
- ensure confidential conversations cannot be overheard;
- position screens to prevent unauthorised viewing;
- lock devices when temporarily unattended;
- securely store any printed documents.

Where confidential information is accessed in public places, additional care should be taken to protect privacy.

15. Business Continuity

15.1 Objective

The Council aims to ensure that essential services can continue in the event of equipment failure, cyber attack or other disruption.

15.2 Electronic Records

Official Council records shall be maintained within approved cloud storage wherever possible to reduce dependence upon any single device.

15.3 Equipment Failure

Where the Council laptop becomes unavailable due to hardware failure, theft or cyber incident, the Clerk shall notify the Chairman as soon as practicable.

The Council will seek to restore access to essential records and services as quickly as possible using cloud-based backups and replacement equipment where necessary.

15.4 Loss of Access

Critical passwords, account recovery information and administrative access arrangements should be managed securely to ensure that the Council can continue to operate if the Clerk is unexpectedly unavailable, while preserving confidentiality and appropriate access controls.

16. Data Protection and Confidentiality

16.1 Commitment

Badgers Mount Parish Council is committed to processing personal information lawfully, fairly and transparently in accordance with:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Freedom of Information Act 2000;
- Environmental Information Regulations 2004;
- Privacy and Electronic Communications Regulations (where applicable).

This policy should be read alongside the Council's Data Protection Policy and Privacy Notices.

16.2 Personal Information

Personal information shall only be:

- collected where there is a lawful basis;
- used for legitimate Council purposes;
- kept accurate and up to date;
- retained only for as long as necessary;
- protected against unauthorised access or disclosure.

Only the minimum personal information necessary to perform Council functions should be processed.

16.3 Confidentiality

Councillors and the Clerk may have access to confidential information in the course of their duties.

Examples include:

- staffing matters;
- complaints;
- legal advice;
- commercially sensitive information;
- planning enforcement information;
- personal information relating to residents.

Such information must not be disclosed except where authorised by law or by the Council.

The obligation of confidentiality continues after a Councillor leaves office or an employee leaves the Council.

16.4 Secure Disposal

Electronic records containing confidential or personal information shall be securely deleted when they are no longer required in accordance with the Council's Records Retention Policy.

Paper documents containing confidential information should be shredded or disposed of through confidential waste arrangements.

17. Freedom of Information and Records Management

17.1 Official Records

Electronic records created or received in connection with Council business are official Council records.

This includes records held within:

- Council email accounts;
- approved cloud storage;
- the Council laptop;
- electronic meeting systems;
- any approved Council applications.

17.2 Councillors' Records

Information relating to Council business may be subject to disclosure under the Freedom of Information Act or Environmental Information Regulations, regardless of where it is stored.

Councillors should therefore ensure that Council business is conducted through their Council email accounts wherever possible and avoid retaining unnecessary copies on personal devices.

17.3 Records Management

The Clerk is responsible for maintaining the Council's official electronic records in accordance with the Council's Records Retention Policy.

Documents should be retained only for the periods specified within that policy.

18. Social Media

18.1 Official Accounts

Only persons authorised by the Council may administer official Council social media accounts or websites.

Login credentials shall be retained securely by the Clerk.

Where appropriate, the Chairman should also know how access can be recovered in an emergency.

18.2 Personal Social Media

Councillors remain free to express personal opinions.

However, when using personal social media they should:

- avoid giving the impression that they are speaking on behalf of the Council unless authorised to do so;
- distinguish clearly between personal and Council views;
- avoid publishing confidential Council information;
- remain mindful of the Councillors' Code of Conduct and the Nolan Principles.

18.3 Respectful Communication

Users should communicate respectfully and professionally.

Online behaviour should reflect the standards expected of elected members and officers.

Content that could reasonably damage the reputation of the Council, disclose confidential information or breach data protection legislation should never be published.

19. Incident Reporting

19.1 Reporting Requirement

Every Councillor and the Clerk has a responsibility to report actual or suspected information security incidents immediately.

Early reporting significantly reduces the potential impact of cyber incidents.

19.2 Examples of Incidents

Incidents include, but are not limited to:

- phishing attacks;
- malware infection;
- ransomware;
- loss or theft of devices;
- accidental disclosure of personal information;
- sending information to the wrong recipient;
- compromised passwords;
- unauthorised access to Council information.

19.3 Reporting Procedure

Where an incident occurs:

1. The user should stop using the affected system if appropriate.
2. The Clerk should be informed immediately.
3. If the Clerk is directly affected, the Chairman should be informed immediately.
4. Relevant passwords should be changed without delay.
5. The incident should be documented.
6. The Clerk shall assess whether the incident constitutes a personal data breach and determine whether the Information Commissioner's Office (ICO) or affected individuals require notification.

19.4 Learning from Incidents

Following any significant incident, the Council should consider whether improvements to procedures, training or technical controls are necessary to reduce the likelihood of recurrence.

20. Training and Awareness

The Council recognises that informed users are one of the most effective safeguards against cyber threats.

Accordingly:

- newly elected Councillors should receive guidance on the Council's digital arrangements;
- Councillors should be encouraged to complete relevant cyber security and data protection training;
- the Clerk should keep up to date with developments in cyber security, data protection and information governance through appropriate professional development.

The Council will seek to promote a culture of continuous learning and awareness.

21. Procurement of IT Hardware and Software

21.1 General Principles

Technology purchased by the Council should be:

- appropriate to operational needs;
- secure by design;
- supported by the manufacturer;
- compatible with existing Council systems;
- good value for money.

21.2 Software

The Council should wherever practicable use reputable, well-supported software from trusted suppliers.

Free software should only be used where appropriate security and licensing considerations have been assessed.

21.3 Cloud Services

Where cloud services are used, preference should be given to providers that:

- comply with UK data protection legislation;
- provide appropriate security controls;
- maintain appropriate backup and resilience arrangements;
- support Multi-Factor Authentication.

21.4 Artificial Intelligence Services

Before adopting any AI service for regular Council use, the Clerk should consider:

- data protection implications;
- confidentiality;
- information security;
- contractual terms;
- reliability;
- whether the service is appropriate for local government use.

The Council should ensure that any AI tools used for official business align with its legal obligations and information governance standards.

22. Monitoring and Compliance

22.1 General Principle

Badgers Mount Parish Council trusts its Councillors and the Clerk to use Council information and technology responsibly.

As a small parish council, the Council does **not** routinely monitor internet activity, email content or the use of personal devices.

However, the Council reserves the right to investigate suspected misuse of Council information or systems where there is a legitimate reason to do so and where such action is lawful, necessary and proportionate.

22.2 Council-Owned Equipment

Council-owned devices and Council-managed electronic records may be examined where reasonably necessary to:

- investigate a suspected security incident;
- recover Council records;
- respond to a Freedom of Information request or legal disclosure;
- investigate an alleged breach of Council policy;

- ensure continuity of Council business.

Any such access shall be authorised by the Council or, where appropriate, by the Chairman in consultation with the Clerk, and shall comply with the UK GDPR and the Data Protection Act 2018.

22.3 Personal Devices

The Council will not seek access to Councillors' personal devices except where:

- Council information held on that device is required for a lawful purpose;
- the Councillor has agreed to provide access; or
- disclosure is required by law.

Where Council information is accessed on personal devices, only information relating to Council business may be relevant to any lawful request.

22.4 Compliance

Compliance with this policy is a condition of access to Council information and systems.

All users are expected to familiarise themselves with the policy and to seek advice from the Clerk where any uncertainty exists.

23. Breaches of this Policy

Failure to comply with this policy may expose the Council to:

- cyber attack;
- financial loss;
- legal liability;
- reputational damage;
- breaches of data protection legislation.

Examples of breaches include:

- sharing passwords;
- disclosing confidential information without authority;
- using Council information for personal purposes;
- installing unauthorised software on Council equipment;
- knowingly introducing malicious software;
- using personal email for Council business without forwarding records to the Council account;

- repeatedly ignoring security advice.

Where a breach is identified, the Council will consider the circumstances and determine any appropriate action.

For employees, this may include action under the Council's disciplinary procedures.

For Councillors, the matter may be considered under the Members' Code of Conduct where appropriate.

Where criminal activity is suspected, the matter may be referred to the appropriate authorities.

24. Policy Review

This policy shall be reviewed:

- every year;
- following significant legislative changes;
- following major changes to the Council's technology arrangements;
- following any significant cyber security incident.

The Clerk shall monitor developments in:

- cyber security;
- information governance;
- artificial intelligence;
- data protection legislation;
- National Cyber Security Centre guidance;
- Information Commissioner's Office guidance;

and recommend amendments where appropriate.

Appendix A

Password Standard

Badgers

Mount Parish Council follows the recommendations of the National Cyber Security Centre (NCSC).

Users should:

- ✓ Use three random words to create strong passwords.
- ✓ Use a different password for every important account.
- ✓ Enable Multi-Factor Authentication wherever available.
- ✓ Never share passwords.
- ✓ Change passwords immediately if compromise is suspected.

Users should **not**:

- ✗ Re-use passwords.
 - ✗ Use birthdays or family names.
 - ✗ Write passwords where others can see them.
 - ✗ Send passwords by email.
-

Appendix B

Device Security Checklist

Before using a device for Council business, users should ensure that:

- ☐ Device is password or PIN protected.
- ☐ Automatic screen locking is enabled.
- ☐ Operating system is up to date.

- ☐ Security updates are installed promptly.
 - ☐ Anti-malware protection is active (where applicable).
 - ☐ Multi-Factor Authentication is enabled.
 - ☐ Device is not shared whilst Council information is accessible.
 - ☐ Public Wi-Fi is avoided for confidential work.
 - ☐ Lost devices can be reported immediately.
-

Appendix C

Cyber Incident Checklist

If you think something has gone wrong:

STOP

Do not continue using the affected system if this may worsen the incident.

REPORT

Notify the Clerk immediately.

If the Clerk is affected, notify the Chairman.

PROTECT

Change passwords if necessary.

Disconnect affected devices if instructed.

RECORD

Make a note of:

- what happened;
- when it happened;
- what information may have been affected;

- who has been informed.

REVIEW

The Clerk will determine whether:

- the ICO must be notified;
 - affected individuals must be informed;
 - additional security measures are required.
-

Appendix D

Acceptable Use Summary

When using Council information:

Always

- ✓ Use your Council .gov.uk email.
- ✓ Protect confidential information.
- ✓ Lock your device.
- ✓ Report suspicious emails.
- ✓ Keep software updated.
- ✓ Use strong passwords.
- ✓ Enable Multi-Factor Authentication.
- ✓ Store official records in the Council's approved cloud storage.
- ✓ Follow the Council's Data Protection Policy.
- ✓ Ask the Clerk if unsure.

Never

- ✗ Share passwords.

- X Publish confidential information.
 - X Use unauthorised software.
 - X Circumvent security measures.
 - X Use Council information for personal gain.
 - X Enter confidential or personal data into public AI systems.
 - X Ignore suspected cyber incidents.
-

References

This policy has been prepared having regard to:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Copyright, Designs and Patents Act 1988
- Local Government Act 1972
- National Cyber Security Centre (NCSC) guidance
- Cyber Essentials
- Information Commissioner's Office (ICO) guidance
- NALC Information Technology Policy Template (adapted)
- Relevant best practice adopted by other parish councils