Meldon Parish Council – Risk Assessment of Financial and Non-Financial Internal Audit Controls

No.	Internal Controls	Risks identified/potential for improvements/current procedure	Action Required
1.	**Governance**		
1.1 1.1.1	Standing Orders Standing Orders have been adopted setting out the Council's constitution and procedures. They are reviewed at least every four years	Reviewed every four years or when changes or made.	
1.2 1.2.1 1.2.2	Financial Regulations The Clerk is the Responsible Financial Officer with the duties detailed in the Financial Regulations. Financial Regulations have been adopted which set out procedures. They are review at least every four years.	Clerk is RFO, detailed in contract. Reviewed every four years or when changes or made.	
1.3 1.3.1 1.3.2	Assertion 10 The Clerk and Councillors have an email address on a council owned domain name for general correspondence from the public. The Council ensures its website complies with the Web Content Accessibility Guidelines	Gov.uk email addresses set up for the Clerk and Councillors - 2025 with Widescope New website 2025 with Widescope	

	(WCAG) 2.2 AA.		
1.3.3	The Council publishes and maintains a clear accessibility statement, that outlines any accessibility limitations, how to request alternative formats, and a named contact for accessibility issues.		
1.3.4	The Council ensures the website complies with the Public Sector Bodies (Website and Mobile Applications) (No. 2) Accessibility Regulations 2018, where applicable.		
1.3.5	The Council adopts and publishes the Information Commissioners Office (ICO) Model Publication Scheme.		
1.3.6	The Council publishes information as required by the Transparency Code for Small Authorities (for those with turnover under £25,000).		
1.3.7	The Council keeps all financial and governance information up to date and makes it accessible via its website.		
1.3.8	The Council has considered its data protection compliance and is sure that it is fully complying		

	with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018.		
1.3.9	The Council is processing personal data with care and in line with the principles of data protection.		
1.3.10	The Council has implemented an IT Policy covering:	IT & Cybersecurity and Data Protection & Retention Policies approved March 2026, reviewed annually	
1.3.11	Use of email and personal devices for official business.		
1.3.12	Email, document handling, data storage and security protocols.		
1.3.13	Responsibilities of councillors, staff and contractors. The policy provides guidance on cyber security threats such as phishing, and outlines mitigation measures.		
1.3.14	The Council reviews the policy annually and shares it with all relevant parties.		

No.	Internal Controls	Risks identified/potential for improvements/current procedure	Action Required
1.4	Measures to Prevent Fraud and Corruption		
1.4.1	The Council has adopted the NALC Model Code of Conduct.	NALC Model Code of Conduct adopted 2020. Reviewed when changes are made.	
1.4.2	All Councillors sign a Declaration of Acceptance of Office on election or co-option.	Signed after 2025 elections	
1.4.3	All Councillors complete a Register of Interests and provide updated information as appropriate. Copies are held with the Council and Northumberland County Council.	Provided after 2025 elections	
1.4.4	There is an agenda item for Councillor Declarations of Interests on every council agenda.	Agenda item	
1.5	Insurable Risks		
1.5.1	Employers Liability Insurance (this is the only insurance the Parish Council is required to hold through legislation.	Insured through Zurich.	

No.	Internal Controls	Risks identified/potential for improvements/current procedure	Action Required
1.6	External Audit Annual Governance Statement Requirements		
1.6.1	Statement of accounts formally approved by Council.	Presented to Council at the Annual Meeting in May	
1.6.2	Council only does things it has legal power to do and works within appropriate standards and codes of practice which could have a significant effect on the ability of the Council to conduct its business or on its finances.	Council has GPC	
1.6.3	Notice of audit displayed on the 3 Council notice boards to allow electors to inspect accounts as required by The Accounts and Audit Regulations 2015.	Displayed on noticeboards	
	Appropriate steps are taken to deal with matters raised in reports from Internal and External Auditors through agenda items on Parish Council meeting agenda.	Completed as and when required.	

No.	Internal Controls	Risks identified/potential for improvements/current procedure	Action Required
1.7 1.7.1	<u>Proper Booking</u> The cash book is balanced against the bank statements to ensure arithmetically correct when bank statements received. Cash book stored in locked cupboard. Budget/Precept reports are held on the Clerks computer and backed up onto USB flash drive.	Completed monthly All accounts documentation stored in safe location. Backs up made monthly, held securely.	
1.8 1.8.1 1.8.2	<u>Payment Controls</u> A list of payments is prepared for the Parish Council meeting with the invoices also available for inspections. Councillor approve these payments and this is recorded in the minutes. Payments are made via BACS or cheques which are signed by 2 approved councillors or clerk/councillor. VAT is recorded in a separate column in the cashbook. Annual reclaims are made.	Presented at every meeting. VAT reclaims completed in April/May annually	

No.	**Internal Controls**	**Risks identified/potential for improvements/current procedure**	**Action Required**
1.8.3	S137 payments are shown in a separate column in the cashbook.	Council has GPC.	
1.9 1.9.1 1.9.2	<u>Budgetary Controls</u> The Council sets a budget which is approved and recorded in the minutes no later than the January meeting. The Clerk presents a quarterly income and expenditure report to the Council.	 Completed annually Presented at every meeting	
2.0 2.0.1 2.0.2	<u>Income Controls</u> All income is recorded in the cashbook. Northumberland County Council issues a remittance advice which confirms the precept that is paid directly into the Council's bank account.	 Completed monthly Received twice a year: April and September	
2.1 2.1.1 2.1.2	<u>Payroll Controls</u> The Clerk manages the payroll. The Clerk is eligible to be paid travel expenses for any official	 The council uses HMRC PAYE Basic Tools. Completed monthly by the Clerk. Claimed annually at the March meeting	

	mileage.		
No.	**Internal Controls**	**Risks identified/potential for improvements/current procedure**	**Action Required**
2.2 2.2.1 2.2.2 2.2.3	<u>Asset Controls</u> An asset register with insurance valuation updates annually. The list of assets is maintained and updated during the year, insurance cover extended for new acquisitions when appropriate. Copy presented to Councillors with annual statement of accounts. Insurance provider reviewed from time to time for competitive pricing.	 Updated as and when required. Completed annually	
2.3 2.3.1 2.3.2 2.3.3	<u>Bank Reconciliation</u> The bank account is reconciled by the Clerk. Quarterly bank reconciliations are undertaken by the Clerk and signed off on the bank statements. Any adjustments for interest/bank charges/unpaid cheques are noted in the cashbook if they occur.	 Completed annually Completed annually Completed annually	

No.	Internal Controls	Risks identified/potential for improvements/current procedure	Action Required
2.4 2.4.1 2.4.2 2.4.3	<u>Year End Procedures</u> Accounts are prepared on a payment and receipts basis. Full cross casting of the cashbook is agreed to the final accounts. The Chairman signs the cashbook. An audit trail is provided by recording the minute number and meeting date the payment was agreed.	Year end accounts completed in April annually Carried out at the Annual Meeting. Completed monthly	
2.5 2.5.1	<u>Qualifications of the Clerk</u> The Clerk holds CilCA (Certificate in Local Council Administration) and is a member of the Institute of Local Council Management.	Completed in 2016. Clerk also has FiLCA and PiALC qualifications.	
2.6 2.6.1	<u>Meetings</u> The meeting policy is set out in Standing Orders, notices are provided three clear days before the meeting on noticeboards. Draft minutes are published prior to the next meeting, time is	Six meetings per year. Notices on website and notice boards 3 days clear Draft minutes published within one month	

	set aside for public participation.		

No.	Internal Controls	Risks identified/potential for improvements/current procedure	Action Required
2.7 2.7.1 2.7.2 2.7.3	<u>Communications</u> The Parish Council has a website Widescope. The Parish Council has an email address that is widely published on noticeboards, emails and websites. Parish Council information is placed on the noticeboards and updated as and when required.	 New website in place from 2025, hosted by Widescope. Gov.uk email address for clerk and councillors from 1st April 2026. Info placed on noticeboards by councillors as and when required.	
2.8 2.8.1	<u>Annual Report</u> Annual Report is completed and published by 30th June of the following year. It is available to any elector and includes a summary of accounts and the Chairman's overview and is presented at the Parish Council meeting.	 Annual Report presented by the Chairman at the Annual Assembly.	

No.	Internal Controls	Risks identified/potential for improvements/current procedure	Action Required
2.9 2.9.1	<u>Accounts</u> Accounts are prepared in accordance with statutory requirements, approved within three months of the accounting date and published within six months.	Accounts updated monthly, presented at each quarterly meeting and published on the website with the agenda for the meeting.	
3.0 3.1	<u>Clerk's Contract</u> The Parish Council has adopted the national Association of Local Council's terms and conditions and contract of employment.	Clerk has NALC model contract.	
3.1 3.1.1	<u>Training</u> The Council has evaluated and identified training needs for staff and members.	Training as and when required	
3.2 3.2.1 3.2.2	<u>General Power of Competence</u> Two thirds of vacancies filled at last election. Clerk is CilCA qualified and has passed unit 7 – General Power of Competence.	Two third of vacancies filled at election 2025. Clerk CiLCA qualified 2016 (includes unit 7 – GPC)	

MITFORD PARISH COUNCIL

DRAFT IT & CYBERSECURITY POLICY

Approved:

1. INTRODUCTION

1.1 Mitford Parish Council has a duty to ensure the proper security and privacy of its computer systems and data. All users have some responsibility for protecting these assets.

1.2 The Parish Clerk/RFO is responsible for the implementation and monitoring of this policy but may delegate that responsibility to another officer.

GENERAL PRINCIPLES

1.3 All employees, members and other users should be aware of the increasingly sophisticated scams and risks posed to cybersecurity, and when in doubt should seek guidance from the Parish Clerk/RFO. As a general rule, users will never be asked to share passwords by email and should be aware of odd language used in emails which may indicate a fraudulent email.

1.4 All employees, members and other users of council IT equipment must be familiar with and abide by the regulations set out in the council's Data Protection & Retention Policy.

1.5 All council devices will have up-to-date antivirus software installed and this must not be switched off for any reason without the authorisation of the Parish Clerk/RFO.

1.6 All users are reminded that deliberate unauthorised use, alteration, or interference with computer systems, software or data is a breach of this policy and in some circumstances may be a criminal offence under the Computer Misuse Act 1990.

1.7 All software installed on council devices must be fully licensed and no software should be installed without the authorisation of the Parish Clerk/RFO.

TRAINING & GUIDANCE

1.9 All users will be provided with regular cybersecurity training as is appropriate for their role and level of systems access.

GENERAL IT POLICY

2.1 All users will be assigned a council email address as appropriate, and this must be used for all council business.

2.2 Members are reminded that an email sent or received in their capacity as a Parish Councillor is council data and any emails must be disclosed following

requests under the Data Protection Act or Freedom of Information Act. This includes emails on personal accounts when acting as a councillor.

2.3 A copy of all emails received are kept in line with the council's Data Protection and Retention Policy.

2.4 The council reserves the right to monitor all activity on council devices. This includes monitoring of logging in and out, email activity and internet usage for the purposes of ensuring compliance with our policies and procedures and ensuring compliance with the relevant regulatory requirements. Information acquired through such monitoring may be used in disciplinary proceedings. Monitoring usage will mean processing personal data.

2.5 Members using social media in their capacity as a councillor must make it clear that they are speaking in a personal capacity, not representing the view of the council.

2.6 Members should ensure they are adhering to the council's Code of Conduct when using social media.

2.7 Members must ensure that any personal devices used to access council systems (including email, websites and data) are password protected and access is restricted solely to the member.

WEBSITES AND SOCIAL MEDIA

3.1 The Parish Clerk/RFO shall ensure that any websites operated by the council are regularly reviewed to ensure content is accurate and up-to-date. Websites shall also be monitored for unauthorized access and abuse.

3.2 Council social media accounts will be operated by the Parish Clerk/RFO.

3.3 All social media messages must be non-political, uncontroversial and used to promote/highlight the parish.

3.4 Approval must be obtained from the Parish Clerk/RFO prior to the creation of any council website or social media account.

PASSWORD PROTECTION

4.1 All council computers and systems must be password protected to prevent unauthorised access.

4.2 Where possible, two factor authentication must be used.

4.3 Users should ensure that unattended devices are password protected and locked when not in use or left unattended.

4.4 Passwords must conform to the following criteria:

- Minimum of eight characters
- Comprise at least one upper case letter, one lower case letter, one number and one special character

4.5 Where possible, generic user accounts should be avoided.

4.6 Where users have unique access permissions and/or accounts for systems, these permissions must not be shared with other users.

4.7 Different passwords should be used for different devices and accounts.

4.8 Passwords must be routinely changed.

4.9 Passwords should not be written down or left in unsecure locations.

PORTABLE DEVICES

5.1 All portable devices (including tablets and mobile phones) must be protected to prevent unauthorised access. This can be by use of passwords, passcodes or other biometric measures as applicable.

5.2 Passcodes must be appropriate for the device and the level or risk that unauthorised access poses to the council; where devices can access personal data or other systems, passcodes must be unique and not easily guessable.

5.3 Particular care must be taken when using removable media to transmit data as such media are easily lost or intercepted. Any sensitive information (including personal data, confidential documents or data which could impact on the rights or reputation of any person or organization, including the council) placed on removable media must be suitably protected or encrypted.

INCIDENT REPORTING

6.1 All users must report any incidents which could pose a risk to the council's systems or data security to the Parish Clerk/RFO without delay. This includes but is not limited to:

- Lost devices
- Potential risk arising from phishing emails/websites

- Passwords having been shared
- Unauthorised access to systems

MISUSE OF IT

7.1 IT systems will be monitored for misuse and all misuse is prohibited.

7.2 Misuse includes, but is not limited to:

- Creation or transmission of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
- Creation of material which is designed or likely to cause annoyance, inconvenience or needless anxiety
- Creation or transmission of defamatory material
- Transmission of material which in any way infringes the copyright of another person
- Transmission of unsolicited commercial advertising material to networks belonging to other organisations
- Deliberate actions or activities with any of the following characteristics:
    a. Wasting staff effort or networked resources
    b. Corrupting or destroying other users' data
    c. Violating the privacy of other users
    d. Disrupting the work of other users
- Other misuse of the networked resources by the deliberate introduction of viruses/malware
- Playing games during working hours
- Altering the set up or operating perimeters of any computer equipment without authority

7.3 Unauthorised access, use, destruction, modification and/or distribution of council information, systems or data is prohibited.