Proposed IT Policy – explanatory covering letter

To: Parish Clerk, Quatt Malvern Parish Council

Subject: Suggested replacement of the November 2025 IT Policy

Dear Bill,

Thank you for forwarding the draft IT Policy. I have reviewed it from the perspective of the Council's internal governance and the practical needs of a small parish council. I enclose a complete proposed replacement, suitable for the Council to consider for adoption. My intention is to retain the useful safeguards in the NALC/WorkNest model while avoiding provisions that may not describe how Quatt Malvern actually operates.

Principal changes and reasons

1. Tailored scope and accountability

The original contains references to servers, dedicated IT providers, offices, continuous monitoring and employment processes that may not apply. The replacement specifies the Clerk's council-owned laptop, councillors' official email accounts and clear responsibility for implementation.

2. Official .gov.uk email accounts

All councillors have been allocated official accounts, although some have yet to activate or adopt them. The replacement establishes official email as the normal channel after training, with a documented temporary exception if necessary. This improves continuity, security and access to Council records.

3. Passwords and MFA

The replacement retains strong passwords and recommends three random words, but removes conflicting requirements to share social media passwords. MFA is required wherever supported, with documented exceptions. Emergency access is arranged without distributing personal passwords.

4. Personal devices

Councillors may reasonably use their own phones and computers to access Council email. The replacement applies straightforward security conditions rather than asserting broad rights to inspect or seize private devices.

5. Backups and business continuity

The original refers to backups without identifying a practical arrangement. The replacement requires Council-controlled storage, a documented backup and recovery process, and contingency access if the Clerk or laptop becomes unavailable.

6. Security incidents and breaches

A clear, prompt reporting route has been added. It distinguishes ordinary cyber incidents from personal data breaches requiring assessment under UK data protection legislation.

7. Monitoring and privacy

The original states that usage is continually monitored and relies on a general legitimate-interests assertion. The replacement avoids claiming monitoring that may not occur and requires any monitoring to be lawful, necessary, transparent and proportionate.

8. Social media and records

The original social media provisions are extensive, occasionally contradictory and may intrude into lawful private expression. The replacement focuses on official publishing, confidentiality, records, the Code of Conduct and account security.

9. Removing obsolete or impractical wording

Detailed provisions about internet cafés, dongles, webcams, extensive disciplinary procedures, automatic wiping of personal devices and Council ownership of personal professional contacts have been removed or replaced with proportionate requirements.

10. Implementation and review

The replacement adds a simple record of account activation, training and policy acknowledgement, with an annual review and incident-triggered review.

Practical recommendations before adoption

- Complete the planned training and confirm that each councillor can access their .gov.uk email account and has enabled MFA where available. Agree a realistic date from which official accounts must be used for all Council business.
- Confirm who administers the .gov.uk email service, website and any cloud storage; record the provider, authorised administrators, recovery methods and support contacts in a secure internal register.
- Check whether the Clerk's laptop has full-disk encryption, supported software, current updates, malware protection and a reliable backup arrangement.
- Identify the authoritative location for Council minutes, correspondence, financial records and other key files; check that backups are recoverable and that authorised continuity access is possible.
- Confirm whether councillors access email on personal devices, and provide a short practical guide to device locking, software updates, MFA and avoiding personal email forwarding.
- Ensure the IT Policy is consistent with the Council's Data Protection Policy, Subject Access Policy, records retention arrangements and any website/publication policies.

Points to confirm

The draft replacement deliberately does not assume that the Council employs an external IT provider, operates central servers, continuously monitors email or has a particular cloud backup service. Those details should be checked and, where necessary, recorded in a short internal operating note rather than making unsupported claims in the public policy.

Legal requirements versus good practice

The Council must implement appropriate security for personal data, handle reportable breaches correctly and comply with its wider legal duties. By contrast, the precise choice of password manager, backup product, training register and device management arrangements is a matter for proportionate local judgement. MFA, secure backups and account continuity are strong security recommendations; the draft policy makes them operational expectations without suggesting that every technical choice is prescribed by statute.

References (for Bill)

Information Commissioner's Office (ICO): UK GDPR guidance on security, personal data breaches and employee monitoring – ico.org.uk

National Cyber Security Centre (NCSC): Small Organisations Guide; guidance on passwords, MFA and backups – ncsc.gov.uk

National Association of Local Councils (NALC): model IT policy and relevant sector guidance (subject to Council tailoring).

I hope these suggestions are helpful. The proposed replacement is intended to be practical, proportionate and straightforward for the Council to administer, rather than an additional burden. I would be happy to discuss any provisions before the policy is put to the Council.

Kind regards,

Steve Jones
Internal Auditor