Briefing for FGP25:61

Risks of a Parish Council Using an Individual's Personal Microsoft 365 Account

Background

When the current Clerk started over 5 years ago there was no regular or automatic backup process for the Parish Council's records or data. To resolve this in the short term, the Clerk used his own cloud storage via his own Microsoft 365 subscription. This was only intended to be an interim solution. This arrangement introduces significant governance, security, accessibility, and compliance risks. It is no longer considered acceptable practice under modern data protection, transparency, and information-governance expectations.

1. Risks Associated with Using a Personal MS365 Account

1.1. Data Access and Ownership

- Parish Council files are stored in a private, individual-controlled account.
- Only the account owner (e.g., the Clerk) has guaranteed access.
- Councillors, auditors, and future staff may not be able to retrieve essential records.
- If the individual is sick, suspended, leaves post, or becomes unable to provide access, the Council may lose operational continuity.

1.2. Succession and Continuity Risks

- Transferring many years of Council records from a personal account is complex and can be incomplete.
- There is no formal guarantee that all documents will be preserved or migrated correctly.
- The Council cannot enforce a retention schedule or archive process on a system it does not control.

1.3. Data Protection & Governance (GDPR) Risks

- Personal accounts do not provide the administrative controls required for a public authority.
- There is no organisation-level audit trail for access, sharing, or deletion.
- Data may be stored in locations or services the Council cannot regulate.
- In the event of a data breach, the Council may not be able to demonstrate compliance with UK GDPR or ICO expectations for public bodies.

1.4. Security & Backup Limitations

- Personal MS365 accounts lack enterprise-grade security features such as:
    - Admin-controlled Multi-Factor Authentication (MFA) enforcement
    - Conditional access policies
    - Centralised device management
    - Information-protection labelling
- Backups depend entirely on the individual's settings and cannot be centrally verified.

1.5. Use of Microsoft Copilot / AI Tools

- If Copilot or other AI features are used under a personal subscription:
    - Data processed by AI may not be protected under enterprise-grade "no training, no leakage" guarantees.
    - Prompts and documents could be processed using models without the compliance protections provided by Microsoft's business licences.
    - This creates potential confidentiality and governance risks, especially for sensitive or draft material.

1.6. Transparency and Public Records Compliance

- Councils must be able to produce records under:
    - Audit requirements
    - Freedom of Information (FOI)
    - Transparency Code obligations
- If documents are scattered within a private account, the Council may be unable to locate or produce required evidence.

1.7. Legal and Reputational Risk

- The ICO has previously flagged that public bodies must not store official data in personal accounts.
- Failure to maintain proper control of information can lead to complaints, enforcement action, or reputational damage.

2. Recommendations to Resolve These Risks

2.1. Adopt a Council-Owned Microsoft 365 Business Subscription

Benefits include:

- Council-controlled accounts for Clerk, Councillors, and staff
- Secure OneDrive and SharePoint storage
- Enforced MFA and security policies
- Central admin control and audit trails
- Full Copilot enterprise compliance (if adopted)

2.2. Create a Dedicated SharePoint Structure

- A SharePoint site for Parish Council records
- Role-based access for Councillors, Clerk, RFO, committees
- Proper separation of confidential and public files
- Automatic versioning and backup

2.3. Migrate Data Out of the Personal Account

- Use Microsoft migration tools or manually transfer content to new Council-controlled libraries
- Document the process and maintain an audit record
- Ensure the personal account retains no residual Council data

2.4. Policies generally required

- Data Management & Retention Policy which WMPC have
- Information Security Policy. An IT policy has been prepared for the Full Council to approve in March
- Acceptable Use & BYOD Policy. This is covered by the Data Management policy and the IT policy
- AI Use Policy (especially for Copilot). This needs to be addressed

2.5. Formalise Succession Planning

- Admin access must be held by the Council, not a single officer
- At least two councillors or authorised officers should have admin rights
- Documentation on system structure and processes should be retained centrally

2.6. Costs

- IT services at CAS manage WMPC website platform, domain and emails. They can provide an appropriate Business Standard license at a cost of £17.50 per month per license. WMPC would need two licenses, one for the Clerk and one for the Deputy Clerk.

3. Conclusion

Relying on an individual's personal MS365 account places Parish Council information at unacceptable risk. It weakens security, continuity, transparency, and governance compliance. Moving to a Council-owned Microsoft 365 business environment ensures proper control, secure storage, and responsible use of AI tools like Copilot. This shift protects the Council, staff, and residents while enabling modern, resilient working practices.