Report: Access to Town Council Emails on Personal Mobile Devices

1. Introduction

Currently, councillors are issued tablets to access their Town Council email accounts and shared files. Councillors have raised concerns about missing important emails as they have not had the tablet to hand or An alternative approach is to allow councillors to access Outlook on their own mobile phones for email only, while continuing to use council-issued tablets for accessing the shared drive. This report sets out the advantages and disadvantages of such a change, along with key security considerations.

2. Advantages of Using Personal Mobile Devices for Email

- Convenience – councillors can check emails quickly on the device they carry daily.
- Faster response – emails are more likely to be read and answered promptly.
- Less reliance on tablets – tablets are only needed when accessing shared files.
- Cost savings – reduced need to maintain tablets solely for email purposes.
- User familiarity – councillors are already comfortable using their own phones.

3. Disadvantages and Risks

- Security risks – council emails may be less secure on personal phones if safeguards are not in place.
- Limited oversight – IT cannot easily enforce updates or remotely wipe a councillor's personal device.
- Data protection – greater risk if phones are lost, stolen, or shared with family.
- Support challenges – multiple phone models and systems may complicate troubleshooting.
- Split usage – councillors must remember to switch to tablets for shared files, which could be inconvenient.

4. Security Safeguards

Since only email access is proposed, risks are lower than full file access, but the following controls are essential:

4.1 Technical Measures

- Multi-Factor Authentication (MFA) – required for all email accounts.
- Outlook app only – restrict access to the official Microsoft Outlook app, not generic mail apps.
- Conditional access – configure accounts so emails cannot be downloaded or stored outside Outlook.
- Device security – require password/PIN, fingerprint/face ID, and encryption on all devices.

- Remote wipe – enable the ability to remotely remove council email data if a device is lost.

4.2 Policy & Governance

- Bring Your Own Device (BYOD) email policy – councillors sign an agreement covering responsibilities.
- Requirement to report lost/stolen phones immediately.
- Agreement not to forward council emails to private accounts.
- Training – short guidance session on phishing risks, safe use, and reporting incidents.

5. Risk Matrix

Risk Area	Tablets Only		Personal Mobiles for Email		Notes / Mitigations
	Likelihood	Impact	Likelihood	Impact	
Data breach (lost/stolen device)	Low	High	Medium	High	Remote wipe and PIN/biometric lock reduce risk.
GDPR compliance breach	Low	High	Medium	High	Strong BYOD policy, training, and technical safeguards needed.
Phishing / malware	Low	Medium	Medium	Medium	MFA, Outlook app, and training mitigate.
Device misuse (family/shared use)	Low	Low	Medium	Medium	Require PIN/biometric and clear councillor responsibility.
IT support burden	Medium	Medium	Medium-High	Medium	Variety of personal devices increases complexity.
Councillor responsiveness	Medium	Low	Low	Low	Faster responses with mobile access.
Cost to council	Medium	Medium	Low	Low	Fewer tablets required only for shared drive.

Risk Ratings (Summary)

- Tablets only – lower risk, but less convenience and higher equipment costs.
- Personal mobiles (email only) – slightly higher security/data protection risks, but manageable with safeguards, and offers better convenience and lower cost.

6. Options

- Continue with tablets only – most controlled, but less convenient.
- Allow personal mobile devices for email only (with safeguards) – balance of convenience and risk.
- Hybrid approach – councillors may choose to stick with tablets for email if preferred.

7. Conclusion

Allowing councillors to access Town Council emails via Outlook on their personal mobile phones could improve convenience and responsiveness, while tablets remain the secure platform for accessing shared files. The approach is viable if technical safeguards (MFA, Outlook app, remote wipe) and a BYOD policy are implemented to ensure GDPR compliance and protect council data.