BROCKLEY PARISH COUNCIL

Councillor Email & Confidentiality Policy

Adopted March 2026 (Next Review June 2027)

1. Purpose

This resource provides a practical standard for councillor email use, helping councils meet the requirements of Assertion 10, uphold confidentiality duties under the Code of Conduct, and ensure secure, auditable communication.

2. Why Councillors Must Use Council-Managed Email Accounts

- Ensures the council retains control of data.
- Allows lawful FOI/SAR searching.
- Enables retention and deletion rules.
- Supports confidentiality and minimises accidental disclosure.
- Ensures accounts can be closed when councillors leave.
- Prevents data being stored across unmanaged devices or cloud services.

3. Minimum Email Standards for Councillors

Councillors should adhere to the following minimum standards when handling council-related information:

- Use only the council-issued email address for council business.
- Do not forward council emails to personal accounts.
- Do not use WhatsApp, SMS, Facebook Messenger or similar apps for casework.
- Enable Multi-Factor Authentication (MFA) on all devices accessing council email.
- Ensure devices used to access council email have a PIN / password lock.
- Avoid downloading attachments to personal devices unless essential.
- Report lost devices or accidental disclosures immediately to the Clerk.

4. Confidentiality Requirements

Under the Code of Conduct, councillors must not disclose confidential information acquired in their role. This includes:

- Personal data (names, contact details, complaints, planning representations).
- Sensitive or special category data (health, allegations, vulnerabilities).
- Financial or commercial information.
- Staffing matters or exempt agenda items.

Confidential information must only be stored within the council-managed email system and must not be shared, forwarded or discussed outside appropriate council processes.

5. Device and BYOD Requirements

- Councillors may access email on personal devices only if security controls are in place.
- Auto-syncing of email content to cloud photo libraries or backup services must be prevented.
- Devices must not be shared with family members.
- Councillors should avoid printing confidential material unless necessary and secure.

6. Joiners–Movers–Leavers (JML) Process

The following steps must be followed when councillors join, change roles, or leave office:

- Account created by Clerk or IT administrator.
- Standards and confidentiality briefing issued.
- Access reviewed annually.
- Account disabled immediately when the councillor leaves.
- Data archived or transferred according to retention policy.

7. Good Practice Checklist

- Council email used exclusively for council business.
- Inbox and folders organised to support FOI/SAR searches.
- No personal account use for forwarding or storage.
- MFA enabled.
- Confidential information handled only within official systems.
- Annual review completed with Clerk.