ST. MARGARET'S
RAINHAM

Mobile Phone and IT Acceptable Use Policy

1. Purpose of this Policy

1.1 This policy sets out how mobile phones, computers, tablets, email, internet access, and IT systems provided by St Margaret's Church, Rainham are to be used. Its purpose is to ensure safe, lawful, responsible, and appropriate use, protecting individuals, the church, and its reputation.

2. Scope

2.1 This policy applies to:

- All clergy, licensed staff, employees, PCC members, and volunteers;
- Anyone using church-owned devices or accessing church IT systems, networks, email, or data;
- Use of personal devices where they are used to access church systems or data.

3. General Principles

3.1 Church IT and mobile devices are provided primarily for church business and ministry purposes.

3.2 Limited personal use is permitted where it is reasonable, lawful, and does not interfere with work, safeguarding, or security.

3.3 Users are responsible for their conduct when using church IT systems.

4. Fair and Acceptable Use

4.1 Users must:

- Use IT systems in a way that is respectful, lawful, and consistent with the values and mission of the church;
- Comply with all relevant legislation, including data protection, safeguarding, copyright, and equality law;
- Not use church systems in a way that could bring the church into disrepute.

5. Prohibited Use

5.1 Church IT systems and mobile devices must **not** be used to:

- Access, view, download, store, or distribute pornographic, sexually explicit, or indecent material;
- Access the dark web, illegal marketplaces, or anonymising services intended to conceal unlawful activity;
- Access material that is extremist, hateful, abusive, discriminatory, or otherwise unlawful;
- Engage in gambling, illegal downloading, or copyright infringement;
- Harass, intimidate, or harm others.

5.2 Any deliberate access to illegal or inappropriate material may result in disciplinary action and, where appropriate, referral to statutory authorities.

6. Mobile Phone Use and Driving

6.1 Church-provided mobile phones must **not** be used while driving. This includes calls, texting, emailing, social media, or using apps, even if hands-free.

6.2 Phones may only be used when the vehicle is safely parked with the engine switched off.

6.3 Users are responsible for complying with road traffic law at all times.

7. IT Security and Safeguarding

7.1 Users must take reasonable steps to keep church systems secure, including:

- Keeping passwords confidential and not sharing them with others;
- Using strong passwords and changing them when prompted;
- Locking screens when devices are unattended;
- Not allowing unauthorised individuals to use church devices;
- Reporting lost or stolen devices immediately.

8. Downloads, Software, and Updates

8.1 Only authorised software and apps may be installed on church devices.

8.2 Users must not download software, apps, or files from untrusted or unofficial sources.

8.3 Copyrighted material must not be downloaded or shared unlawfully.

8.4 Operating systems, apps, and security updates must be installed promptly when requested.

9. Viruses, Malware, and Antivirus Protection

9.1 Church devices must use approved antivirus and security software.

9.2 Users must not disable or bypass security controls.

9.3 Any suspected virus, malware, or unusual device behaviour must be reported immediately.

10. Email and Link Security

10.1 Users must take care when using email, including:

- Being alert to phishing emails, scams, and suspicious messages;
- Not clicking on unknown or unexpected links or attachments;
- Verifying requests for money, personal data, or login details before responding;
- Reporting suspicious emails to the appropriate church contact.

10.2 No legitimate organisation will ask for passwords or sensitive information by email.

11. Data Protection and Confidentiality

11.1 Personal and confidential information must be handled in accordance with the church's Data Protection Policy.

11.2 Sensitive information must not be stored insecurely or shared without authorisation.

11.3 Church data should only be stored on approved systems and devices.
11.4 Images can only be taken and stored in line with the church's photography policy.

12. Monitoring and Privacy

12.1 The church reserves the right to monitor use of its IT systems where necessary for security, safeguarding, or legal reasons.
12.2 Monitoring will be proportionate and lawful.
12.3 Users should have no expectation of complete privacy when using church systems.

13. Breaches of this Policy

13.1 Failure to comply with this policy may result in:

- Withdrawal of access to IT systems;
- Disciplinary action under relevant church procedures;
- Referral to statutory authorities where required.

14. Review

14.1 This policy will be reviewed periodically and updated as required to reflect changes in technology, law, or church practice.

15. Adoption of this Policy

15.1 The PCC of St Margaret's Church formally accepted this policy at the PCC meeting held on 22 January 2026.