St Mary's Ewell
www.stmarysewell.com

St Mary the Virgin, Ewell – Email Use Policy (2026)

1. Purpose of this Policy

2. Scope

3. Ownership and Use of Church Email Accounts

4. Required Disclaimer

5. Acceptable Use

6. Sensitive or Pastoral Matters

7. Confidentiality and Forwarding

8. Data Protection & GDPR Compliance

9. Security Requirements

11. Behaviour and Conduct

12. Monitoring

13. Breaches of Policy

14. Review

St Mary the Virgin, Ewell – Email Use Policy (2026)

Approved by PCC October 2026

1. Purpose of this Policy

This policy sets out how email is to be used for church business within St Mary the Virgin, Ewell (Registered Charity No. 1128409). Its aims are to:

- Protect personal data and comply with UK GDPR and the Data Protection Act 2018.
- Ensure safe, respectful, and appropriate communication.
- Provide clarity for clergy, staff, volunteers, and PCC members.
- Maintain consistent use of official church email accounts.

2. Scope

This policy applies to:

- Clergy, staff, PCC members, volunteers, and anyone acting on behalf of St Mary's.
- All communication sent using **@stmarysewell.com** email addresses.
- Any personal devices used to access church email accounts.

3. Ownership and Use of Church Email Accounts

- Church email accounts are provided **solely for church business**.
- Church role holders must not use personal email accounts for Church business, unless in times of emergency.
- Users must not use church email accounts for personal commercial activity or political campaigning.
- Limited personal use is acceptable only if it does not interfere with church duties and complies with this policy.
- All emails sent from church accounts may be retained for administrative, safeguarding, or legal purposes.

4. Required Disclaimer

All church email accounts **must** include the following disclaimer in the signature block:

This message contains information sent on behalf of (insert name) a member of the PCC of St Mary the Virgin Ewell (registered charity no 1128409), and may include privileged and confidential information. Emails and email addresses may be kept. If you believe you are not the intended recipient you may not make any disclosure, distribution or use of contents. If you have received this message in error please delete and notify the sender immediately.

This disclaimer must not be altered without PCC approval.

5. Acceptable Use

Email may be used for:

- Circulating agendas, minutes, rotas, notices, and administrative documents.
- Coordinating/ participating in events, meetings, and volunteer activities.
- Pastoral communication where appropriate (but see Section 6).

- Sharing information necessary for the functioning of church groups and ministries.
- Where it is likely that the personal data received or sent by role holders would be considered sensitive, high risk or special category an email account provided by our email service provider must be used. A personal email account may not be used for this purpose.

Users should:

- Write clearly, kindly, and professionally.
- Allow time for reflection before sending sensitive messages.
- Use "Reply All" sparingly.
- Keep inboxes reasonably organised to support data retention rules.

6. Sensitive or Pastoral Matters

Email is **not** suitable for:

- Complex pastoral conversations.
- Matters likely to cause distress or disagreement.
- Safeguarding concerns (which must follow the Safeguarding Policy and be reported immediately).
- Any sensitive information should be sent in protected attachments.

If an email exchange becomes difficult or contentious, communication should move to:

- A phone call,
- A face-to-face conversation, or
- A meeting.

7. Confidentiality and Forwarding

- Emails are for the named recipient(s) only.
- Do not forward emails containing confidential, pastoral, or sensitive information unless you have explicit permission.
- When forwarding routine business emails, check that no personal or sensitive data is included.

If unsure, ask the sender: *"Would you like me to forward your email to X, or would you prefer to contact them directly?"*

8. Data Protection & GDPR Compliance

In line with UK GDPR requirements for churches :

- Personal data must only be used for legitimate church purposes.
- Email addresses may be retained for administrative, pastoral, or safeguarding reasons.
- Members may request removal from mailing lists; this must be honoured unless a legal obligation requires retention (e.g., Gift Aid records).

Approved by PCC October 2026

- Group emails containing many recipients must use **BCC** unless explicit consent has been given to share addresses.
- Every bulk email must include an unsubscribe or opt-out option where appropriate (e.g., newsletters).
- Data breaches (e.g., sending personal data to the wrong recipient) must be reported immediately to the data protection co-ordinator. dataprotection@stmarysewell.com

9. Security Requirements

All users must:

- Use strong passwords and keep them confidential.
- Enable multi-factor authentication where available.
- Report suspected compromise immediately.
- Not store church emails on unsecured devices or share login details.
- Avoid using public Wi-Fi for accessing church email unless using a secure VPN.

10. Record Keeping and Retention

- Emails may be retained for administrative, legal, or safeguarding reasons.
- Emails containing personal data should be archived or deleted when no longer needed.

11. Behaviour and Conduct

Users must not use church email to:

- Harass, bully, or discriminate.
- Share inappropriate content.
- Circulate rumours or confidential information.
- Engage in any activity that could damage the reputation of St Mary's.

12. Monitoring

In line with UK law on monitoring communications (RIPA 2000 and GDPR) :

- Church email accounts are not private and can be accessed by those given authority by the PCC to access, when authorised, church email accounts.
- Monitoring may occur for security, safeguarding, or legal compliance.
- Users will be informed if monitoring is required.
- In the case of technical problems, there may, very occasionally, be a need to access someone else's emails.
- In the case of sickness, police investigations and like emergencies, there may be a need to access a church email account. This should only be done on the agreement of the Vicar and Churchwardens (or Churchwardens in the absence of the Vicar.) If it is proposed to access the email of a member of the clergy or someone else with pastoral

responsibility (e.g. a pastoral assistant), the bishop should be consulted first, because of the very sensitive and confidential nature of some emails sent on pastoral matters.

- Both the intended recipient and the sender should be informed of how and why emails were accessed in these cases

13. Breaches of Policy

Breaches may result in:

- Withdrawal of email access,
- PCC review,
- Safeguarding referral (if relevant),
- Disciplinary action under the parish's HR or volunteer procedures.

14. Review

This policy will be reviewed annually by the Data protection compliance officer and Churchwardens or sooner if legislation changes.