





St Mary’s Wootton uses digital communication and social media in order to communicate with members of the congregation and to the wider community. Social media is used to communicate and live out the church’s mission of “*knowing Jesus, making Jesus known to all*”. To ensure we keep everyone safe, we have adopted a digital communication and social media policy. This policy will be reviewed annually and was last reviewed by St Mary’s Parochial Church Council (PCC) on 19 January 2026.

Contents

Digital communication and social media policy.....3

 CCPAS e-safety definition.....3

 Safeguarding contact details.....3

Appendix 1: Digital communication at St Mary’s Wootton, as of January 2026.....4

Appendix 2: Specific Guidelines for forms of digital communication..... 5

 Use of Smart Phones.....6

 Taking and publishing photographs and videos or images, including on websites..... 6

 E-mail.....6

 Chat and messenger Services.....6

 Use of WhatsApp for church business..... 6

 Use of social networking sites..... 6

 Responding to concerns..... 6

Digital communication and social media policy

CCPAS e-safety definition

“E-safety – or electronic safety is the collective term for safeguarding involving the use of mobile phones, computers, tablets and other electronic devices including games consoles, to communicate and access the Internet, emails, text messages (SMS), Instant Messaging (IM), social networking sites (SNS) and other social media.”

Below sets out the expectation of digital communication and social media at St Mary's Wootton. When using social media in relation to St Mary's, you agree to:

- Be safe. The safety of children, young people and vulnerable adults must be maintained at all times.
- Be respectful. Do not post or share content that is sexually explicit, inflammatory, hateful, abusive, threatening or otherwise disrespectful. The posting of personal views towards the church and its work or its members or staff is prohibited.
- Be kind. Treat others how you would wish to be treated and assume the best in people. If you have a criticism or critique to make, consider not just whether you would say it in person, but the tone you would use.
- Be honest. Don't mislead people about who you are.
- Take responsibility. You are accountable for the things you do, say and write. Text and images shared can be public and permanent, even with privacy settings in place. If you're not sure, don't post it.
- Be a good ambassador. Personal and professional life can easily become blurred online so think before you post.
- Credit others. Acknowledge the work of others and respect copyright.
- Follow the rules. Abide by the terms and conditions of the various social media platforms themselves.

(Adapted from Church of England, social media community guidelines, 2022)

St Mary's officers reserve the right to take down, or request others take down any post that we feel breaches any of these conditions.

With any use of social media or digital communication, confidentiality should always be considered, just as it would be in face-to-face situations. Things of a confidential nature should not be shared on social media. There are many social media platforms, St Mary's only uses approved social media platforms set out on page 3.

Any content or conversations which raises concern should be saved and passed on to the Parish Safeguarding Officer (PSO), Incumbent or Diocesan Safeguarding Adviser (DSA).

Safeguarding contact details

St Mary's Parish Safeguarding Officer		safeguarding@stmaryswootton.org.uk
St Mary's Incumbent / vicar	01234 768391	vicar@stmaryswootton.org.uk
Diocese of St Albans Diocesan Safeguarding Officer www.stalbansdiocese.org/safeguarding/safeguarding-contacts/	01727 818107 07867 350 886	safeguarding@stalbans.anglican.org

Appendix 1: Digital communication at St Mary's Wootton, as of January 2026

Form of communication	Intended users	Administrator	Additional safeguarding processes
Facebook pages / groups (SNS)	Public	Church administrator / Emma Hearn	• Photos of individuals posted with consent. • Direct messaging is turned off. • Closed group for parents / carers / volunteers only. • Direct messaging only happens to communicate key information and there are multiple admins with the ability to read messages.
Instagram accounts (SNS)	Public	Emma Hearn	• Photos only posted with consent. • Admin also has a pastoral role and will follow up any messages of concern. • Only use for people over 16.
WhatsApp groups (IM)	Members of the congregation by their agreement in relation to approved church business		• Members of the group will follow up any messages of concern with a group leader, Incumbent or safeguarding team. • Groups to be only created for the purpose of approved church activities outlined in the safeguarding policy such as growth groups, children's work or working parties. • Only use for people over 18.
Mailchimp (direct email)	Those who sign up to receive bulletins / to specific mailing lists via Mailchimp	Church administrator or approved users	• GDPR complaint – individuals have to sign up and have the ability to unsubscribe themselves should they wish to no longer receive information via Mailchimp.
ChurchSuite	Members of the congregation who have signed up to ChurchSuite.	Church staff team	• GDPR Compliant. • Opt-in with permission via consent form. • Individuals have access to their own ChurchSuite login where they are able to edit their personal information and accessibility. • Individuals can update their privacy settings to determine which information is visible to other My ChurchSuite users. In the same way, other members can only see the information they have chosen to openly share. • No children's data is available to other ChurchSuite users. • Individuals are able to choose how they wish to receive communications from church. • Each individual has their own login and password to ChurchSuite.
YouTube account (SNS)	Public	Martin Sanders	• Closed account. • Restricted who can upload to Youtube. • Used for the purpose of live streaming only.

If a social media type is not listed above, St Mary's PCC does not approve its use for church business.

Appendix 2: Specific guidelines for forms of digital communication

Do:

- Have your eyes open and be vigilant when using social media or digital communication.
- Maintain the utmost integrity – honesty, transparency, consistency and accountability.
- Treat online communication with children, young people and adults as you would communication that is face to face.
- Maintain confidentiality when posting on social media sites, emailing or messaging.
- Report any safeguarding concerns that arise on social media to the PSO, Incumbent or DSA.
- Always assume that everything you write is permanent and may be viewed by anyone at any time; and that everything can be traced back to you personally, as well as to your colleagues or the church.
- Think before you post.
- Draw clear boundaries around your social media usage associated with your private life and your use of different social media for public ministry.
- Keep church account(s) and profiles separate from your personal social media account.
- Always ask parents / carers for written consent to:
 - use and store photographs of children / young people from activities or events in official church publications, or on the church's social media, website and displays.
 - use telephone, text message, email or other messaging services if communicating with people under 18 for the purpose of church business.
- Save any messages and threads through social networking sites, so that you can provide evidence of your exchange if required.
- Use clear and unambiguous language in all communications, and avoid abbreviations that could be misinterpreted.
- Download and save any inappropriate material received through social networking sites or other electronic means and show immediately to the PSO, Incumbent or DSA.
- Use passwords and log off promptly after use to ensure that nobody else can use social media pretending to be you.
- Use an appropriate tone: friendly, but not over-familiar or personal.
- Be warm and friendly, but do not suggest or offer a special relationship.
- Respect a child's / vulnerable adult's right to confidentiality unless abuse / harm is suspected or disclosed.
- Keep your own social media sites secure by ensuring you have adequate privacy settings.

Do not:

- Use a personal social media account for church business.
- Add children, young people or vulnerable adults as friends on your personal accounts even if they request to follow you or be your friend.
- Say anything on social media that you would not be happy saying in a public meeting, to someone's face, writing in a local newspaper or on headed notepaper.
- Share any personal information, or request or respond to any personal information from a child/vulnerable adult other than that which might be appropriate as part of your role.
- Comment on photos or posts, or share content, unless appropriate to your church role.
- Use video communication on a one-to-one basis (unless prior agreement has been sought from supervisor and parents if under 18). Ideally, all video communication should have at least two leaders present.
- Allow content or share links to other sites that contain:
 - Libellous, defamatory, bullying or harassing statements.
 - Breaches of copyright and data protection.
 - Material of an illegal nature.
 - Offensive sexual or abusive references.
 - Inappropriate language.
 - Anything which may be harmful to a child, young person or vulnerable adult, or which may bring the church into disrepute or compromise its reputation.

Use of smartphones

- Staff and volunteers should not give out their personal mobile phone number to children, young people or vulnerable people.

Taking and publishing photographs and videos or images, including on websites

- For any photos that are taken at church events, an opt-out announcement will be made for those who do not wish to appear in photos or have their photographs shared on social media platforms.
- For events where parents or carers are not present, specific permission will be sought.
- Images should only be taken for a specific purpose, such as displaying on St Mary's website and social media platform to promote church business.
- Others should not share photos taken at events on social media without prior consent from individuals.
- Children's full names will not be used anywhere on the website.
- A poster informing individuals the service is being livestreamed will be displayed and individuals will know where they will not be seen on camera.
- Photographs should only be taken by appointed people and they should be uploaded to the secure staff drive or St Mary's Facebook page, with parental permission. They should be deleted on the device as soon as possible.
- Only designated volunteers should take photographs of children unless specific permission is sought.

Email

- Obtain parental agreement before using email services to communicate with a child or young person under 18.
- If emailing people under 18, copy in at least one other leader and parent / carer into all correspondence.
- Use clear, unambiguous language to reduce the risk of misinterpretation (e.g. never use terms such as 'luv').
- Email should only be used to communicate specific information (e.g. times and dates of events). It should not be used as a relationship building tool.
- Where possible, communication should be made via ChurchSuite.

Chat and messenger services

- Chat and messenger services should only be used as a last resort of communication and must be used for communication related to church activities only.
- Messaging should only happen from a church account with multiple leader access and not from a personal account.
- Chat and messenger services should not be used for people under 16.

Use of WhatsApp for church business

- Individual consent should be gained before adding anyone to a group.
- Only people aged 18 and over should be part of a WhatsApp group.
- WhatsApp groups should be monitored by the admins.
- WhatsApp groups may be created without the permission of the PCC as long as it is for the purpose of one of the listed church activities in the safeguarding policy.
- Once a group is no longer needed, the group should be deleted by the admin of the group.
- Disappearing messaging should be disabled.

Use of social networking sites

- If it is necessary to set up a new social media account or page for church business, approval from the PCC should be sought.

Responding to concerns

- Any content or conversations which raise concern should be saved and passed on to the PSO, Incumbent or DSA (contact details on page 3).