

Digital communication and social media Policy

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 St Mary'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 was adopted by St Mary's PCC on 19th February 2024 and will be reviewed annually.

Contents

Digital communication and social media Policy	2
CCPAS e-safety definition.....	2
Expectations of digital communication and social media at St Mary's.....	2
Appendix 1: Digital Communication at St Mary's, Wootton as of June 2022.....	4
Appendix 2: Specific Guidelines for forms of digital communication.....	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.

Expectations of digital communication and social media at St Mary's

Below sets out the expectation of digital communication and social media at St Mary's Wootton. By engaging with St Mary's social media accounts, you agree to:

- **Be safe.** The safety of children, young people and vulnerable adults must be maintained by following guidance in the Parish Handbook. Children and young people will not be added to personal social media accounts of church officers or volunteers. Any concerns relating to the safety of others should be reported to the Parish Safeguarding Officer – Kate Wilson – safeguarding@stmaryswootton.org.uk or to the Incumbent, Peter Ackroyd. If this is not possible these should be passed to the Diocesan Safeguarding Adviser (safeguarding@stalbans.anglican.org/01727818107).
- **Be respectful.** Do not post or share content that is sexually explicit, inflammatory, hateful, abusive, threatening or otherwise disrespectful.
- **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.
- **Disagree well.** Some conversations lead to disagreements, and it is important we apply our values in the way we express the disagreements. Social media is not the place in which to express personal views towards the church and its work or its members or staff.
- **Credit others.** Acknowledge the work of others. Respect copyright and always credit where it is due. Be careful not to release sensitive or confidential information and always question the source of any content you are considering amplifying.
- **Follow the rules.** Abide by the terms and conditions of the various social media platforms themselves. If you see a comment that you believe breaks their policies, then please report it to the respective company or Kate Wilson, Parish Safeguarding Officer or Incumbent.

(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.

Communication between children and vulnerable adults should always take place within clear boundaries; this includes face to face contact, mobile phones, text messaging, emails, digital cameras, videos, webcams, websites, social media sites, and blogs. Using digital communication safely will avoid the risk of

- Forming inappropriate relationships.
- Saying things you should not, such as offensive, sexual or suggestive comments.
- Blurring the boundaries between public work/ministry and your private life.
- Grooming and impersonation.
- Bullying and harassment.

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.

Appendix 1: Digital Communication at St Mary's, Wootton as of January 2024

Form of Communication	Intended Users	Administrator	Additional Safeguarding Processes
Facebook Pages/Groups	Public	Di Murray, Peter Ackroyd, Emma Hearn	<ul style="list-style-type: none"> • 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. • Photos only posted with consent.
Instagram Accounts	Public	Di Murrey/Emma Hearn	<ul style="list-style-type: none"> • Photos only posted with consent. • Admin also has a pastoral role and will follow up any messages of concern. • WhatsApp age restriction is 16+
WhatsApp Groups	Members of congregation by their agreement in relation to approved church business.		<ul style="list-style-type: none"> • Members of the group will follow up any messages of concern with 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 over 18's
Mail chimp	Those who sign up to receive bulletins/to specific mailing lists via mail chimp	Di Murray	<ul style="list-style-type: none"> • GDPR compliant – individuals have to sign up and have the ability to unsubscribe themselves should they wish to no longer receive information via mail chimp.
Church suite	Members of the congregation who have signed up to church suite.	Di Murray Church staff team	<ul style="list-style-type: none"> • GDPR Compliant • Opt in with permission via consent form • Individuals have access to their own church suite log in 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 Church Suite users at St Mary's Wootton. In the same way,

			<p>individuals can only see the information that they choose to make visible in their privacy settings.</p> <ul style="list-style-type: none"> • No children's data is available to other church suite users. • Individuals are able to choose how they wish to receive communications from church. • Each individual has their own login and password to church suite.
YouTube Account	Public	Martin Sanders	<ul style="list-style-type: none"> • Closed account • Restricted who can upload to you tube • Used for the purpose of live streaming only.

Appendix 2: Specific Guidelines for forms of digital communication

General Guidelines for digital communication for staff and volunteers adapted from 'The Parish Safeguarding Handbook, 2018.

Do:

- Have your eyes open and be vigilant.
- Maintain the upmost 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 Parish Safeguarding Officer or Diocesan Safeguarding Advisor in their absence.
- 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/s e.g. only use a Facebook page, Twitter or blogs for public ministry, while keeping a separate Facebook profile for private life.
- 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 and other messaging services to communicate with young people.
 - Allow young people to connect to the church's social media pages.
- Only use an approved church account to communicate with children, young people and/or vulnerable adults. The named person should be able to access this and review conversations, and the account should be visible to young people and their parents. Young people must be made aware that any communication will be viewed by all users.
- Save any messages and threads through social networking sites, so that you can provide evidence to the named person of your exchange when required.
- Avoid one-to-one communication with a child or young person.
- Use clear and unambiguous language in all communications and avoid abbreviations that could be misinterpreted.
- Save and download to hard copy any inappropriate material received through social networking sites or other electronic means and show immediately to Kate Wilson, Parish Safeguarding Officer safeguarding.saintmarys@gmail.com or Peter Ackroyd incumbent or, if appropriate, Diocesan Safeguarding Adviser.
- 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.
- Be clear and explicit about information that you need to share; don't abbreviate or short-cut your communications.

- Be clear and open about your communications with children or vulnerable adults to avoid any possible misinterpretation of your motives or any behaviour which could be construed as grooming.
- Maintain good and open relationships with vulnerable adults and parents and carers
- Only make contact with children for reasons related to the work of the church and maintain a log of all electronic contact with individuals or groups including messaging and texting. Where possible use only equipment provided by the church to communicate with children.
- 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 had adequate privacy settings.

Do not:

- Use a personal Facebook or any other social media account in your work with children, young people or vulnerable adults.
- Add children, young people or vulnerable adults as friends on your personal accounts even if they request to follow you or be your friend.
- Stalk social media sights to find out information about individuals.
- 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 visual media (e.g. Skype, Facetime) for one-to-one conversations with young people – use only in group settings.
- Allow content to contain 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 video communication on a 1:1 basis unless prior agreement has been sought from supervisor and parents. Ideally all video communication should have at least 2 leaders present.

Use of Smart Phones

- Staff and Volunteers should not give out personal mobile phone number to children and young people.
- Photographs taken using a smart phone should only be taken by a staff member and uploaded to the secure staff drive or St Mary's Facebook page with parental permission at the earliest opportunity and deleted from phone straight afterwards.
- Volunteers should avoid taking photographs of children on their phone at all times.
- Any communication of concern should be reported to the Parish Safeguarding Officer – Kate Wilson or the incumbent Peter Ackroyd.

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.
- 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. .
- Children's full names will not be used anywhere on the website in association with photographs.
- A disclaimer will be displayed in church to warn individuals that photos maybe taken in church and used for the purpose of church business.

E-mail

- Obtain parental agreement before using email services to communicate with a child or young person.
- Use clear, unambiguous language to reduce the risk of misinterpretation (e.g. terms such as 'luv' to round things off should never be used).
- Copy in at least 1 other leader/parent into all correspondence.
- 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 church suite
- Any conversations that raise concerns should be saved and passed on/shown to the Parish Safeguarding Officer or Peter Ackroyd, Incumbent.

Chat & Messenger Services

- Chat and messenger services should only be used as a last resort of communication for church business only.
- Where contact is made to you via messenger services, advise the person email.
- 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 under 16's.
- Communication will not take place after gpm.
- Any conversations that raise concerns should be saved and passed on/shown to the Parish Safeguarding Officer or Peter Ackroyd, Incumbent.

Use of WhatsApp for church business (review this when reviewing policy)

- Individual consent should be gained before adding anyone to a group. Only young people age 18 and over should be part of a WhatsApp group.
- WhatsApp groups should be monitored by the admins
- Whats App groups maybe 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.

- The group leader should be an admin for the group and where appropriate a member of staff
- Any concerns should be reported to Parish Safeguarding Lead, or Peter Ackroyd, Incumbent.

Use of social networking sites

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

Responding to concerns

Any content or conversations which raises concern should be saved and passed on to the Kate Wilson, Parish Safeguarding Officer – safeguarding.saintmarys@gmail.com or Peter Ackroyd, incumbent. If this is not possible these should be passed to the Diocesan Safeguarding Adviser -safeguarding@stalbans.anglican.org/01727 818107