



St Stephen's and St Wulstan's
knowing Jesus + making Jesus known

Use of Social Media

This policy was agreed by St Stephen's and St Wulstan's PCC at their meeting held on **24th March 2026**.

It will be reviewed annually.

Version Control:

Version no.	Drafted	Adopted
2025.1	January 2025	25 th March 2025
2026.1 MAJOR REVISION	March 2026	24 th March 2026

The PCC of St Stephen's and St Wulstan's agree to comply with the guidance given on the Safeguarding Dashboard.

Therefore, the PCC of St Stephen's and St Wulstan's agree to:

- Follow the Church of England's national guidance regarding the use of social media (Safer Environment and Activities – Section 4, 2019)
- Approve all official uses of social media for its activities (see **point 1**)
- Ensure that there is a Social Media Co-Ordinator to whom all those who administer or have access to official church accounts are accountable (see **point 2**)
- Ensure that all church officers who use social media on behalf of the church are aware of this policy, especially the risk assessment (see **point 3**).

1. When do these Procedures and Practices apply?

This policy applies to "official" social media accounts that are used for the purposes of the church or its activities. Any such accounts **must be approved** by the PCC.

The PCC considers that these roughly fall into two categories:

1. **External facing.** These are publicly accessible by anyone on the internet. For example, a church YouTube or Instagram account.
2. **Limited access.** These are not publicly accessible and require some kind of invitation to join. This lowers the inherent risk. WhatsApp groups would fall into this category.

This policy does **not** apply to personal accounts that are held by individual church members or church officers, or to WhatsApp groups or similar that include church members but are not clearly linked to an official function or activity of the church (for example, a WhatsApp group for a prayer triplet). Our *Safeguarding Procedures and Practices* includes more information about some restrictions for church officers' use of personal social media accounts.

If a someone becomes aware of a social media account that they believe should be covered by this policy, they should inform the Social Media Co-Ordinator.

2. The Social Media Co-Ordinator

The PCC of St Stephen's and St Wulstan's appoint **Tom Bryant** as Social Media Co-Ordinator.

The Social Media Co-Ordinator will, on behalf of the PCC:

- compile and maintain an up-to-date list of "official" church social media accounts, along with the names of the church members who administer them and those who have access to them
- maintain a list of the login details for each of the **external facing** church social media accounts
- contact all WhatsApp group administrators annually to remind them to post the "Guidelines for Church WhatsApp Groups" and remove any non-active members.

3. Risk Assessment

- Severity levels 4–5 must be reported to the PCC immediately
- Safeguarding concerns must be reported to the Parish Safeguarding Officer
- We define severity across four dimensions:
 - o Reputation
 - o Safeguarding
 - o Legal/data protection
 - o Operational disruption
- The highest impact determines the severity.

Risk Matrix		Risk = Severity x Probability				
Probability	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Severity				

Action Required	
1 - 4 Low Risk	Acceptable/tolerable
5 - 9 Med Risk	Reduce risk to 'as low as reasonably practicable'
10 - 25 High Risk	Unacceptable/Intolerable - activity to stop until risk has been reduced to an acceptable or tolerable level

SEVERITY	SCORE
Minor issue with little or no external impact. Easily corrected. Examples: typo in a post, incorrect event time quickly amended, a single mildly negative comment.	1
Localised issue causing limited reputational impact or short-term confusion. Examples: inappropriate but non-offensive comment posted by mistake, small number of negative comments, temporary account compromise with no harmful content posted.	2
Incident that could cause reputational harm or operational disruption if not addressed promptly. Examples: misleading or inaccurate information posted publicly, inappropriate content shared unintentionally, limited misuse of an account, or exposure of non-sensitive personal information.	3
Serious incident involving significant reputational damage, safeguarding concerns, or potential breach of data protection law. Examples: account hacking used to post offensive content, disclosure of personal data, misuse of church account involving harassment or safeguarding issues. Requires immediate action and possible reporting to authorities.	4
Major crisis with serious legal, safeguarding, or reputational consequences. Examples: large-scale data breach, use of church social media to facilitate abuse or exploitation, significant safeguarding incident involving children or vulnerable adults. Requires urgent PCC-level response and reporting to authorities.	5

PROBABILITY		SCORE
Almost certain	Is expected to occur in most circumstances	5
Very likely	Will probably occur in most circumstances	4
Likely	Will probably occur at some time	3
Unlikely	May occur at some time	2
Extremely unlikely	May occur only in exceptional circumstances	1

Issue/how harm can occur	Example	Current/existing control measures	Risk rating based on existing controls			IMPROVEMENT PROGRAM				
						Additional control measures		RESIDUAL RISK		
			Sev.	Prob.	Risk			Sev.	Prob.	Risk
Inaccurate or misleading information posted	Wrong service time or event information shared	Account administrators should proofread all posts before making them public. If an error is spotted or brought to our attention it will be corrected as soon as possible. The Social Media Co-Ordinator has access to accounts and can correct or delete misleading posts.	1	3	3					
Personal, inappropriate or insensitive content posted by mistake	Volunteer posts a link to a site that includes something political or offensive from the church account. Volunteer posts to a church account rather than personal account by accident.	Account administrators should proofread all posts before making them public. This must include checking the content of any externally linked websites. Volunteers should log out of any church account after they have finished posting. Account administrators are known to the Social Media Co-Ordinator and receive guidance about what is/is not appropriate. The Social Media Co-Ordinator has access to accounts and can delete posts.	2	2	4	It may be appropriate to post an apology if inappropriate/ insensitive content has been posted. Any repeated behaviour will be responded to as a pastoral issue.				
Negative comments escalating	Complaint about church member spreads in comments or a WhatsApp group Negative community responses on a social media post	Settings for comments to be configured so that if they are not necessary, they are disabled. Comments may be locked for a post if needed. Social Media Co-Ordinator can be contacted to advise on moderation if required. Administrators of church WhatsApp groups share guidelines every year.	2	2	4	Any concerns about behaviour to be responded to as a pastoral issue including use of complaints process to address concerns about staff members.				

Key: Sev. = Severity, Prob. = Probability

Issue/how harm can occur	Example	Current/existing control measures	Risk rating based on existing controls			IMPROVEMENT PROGRAM			
			Sev.	Prob.	Risk	Additional control measures	RESIDUAL RISK		
							Sev.	Prob.	Risk
		Administrators of church WhatsApp groups to intervene if unhelpful or unkind messages are being sent. If necessary these can be reported to the Social Media Co-Ordinator.							
Unauthorised/inappropriate people included in closed group chats	Someone briefly attends church and is added to a WhatsApp group, then leave but is still in the group 2 years later, receiving potentially sensitive information.	WhatsApp group administrators reminded annually to check group membership and remove anyone who no longer attends.	2	1	2				
Account compromise or hacking	Social media password acquired and spam links posted	Use strong passwords. Do not leave accounts logged in. Do not leave devices unattended when logged in. Change passwords if account compromise is suspected. Delete all spam posts once account control regained.	3	2	6				
Personal data shared without consent	Photo of a child posted without parental permission	Consent forms for children involved in church activities. Gain/check consent for photographs before taking them. Always check for consent before posting any photograph with children in view. Never name children shown in a photograph or video. Adjust livestream camera angles to avoid accidentally capturing children's images as far as possible. Follow obligations under UK GDPR and the Data Protection Act 2018 if there is a breach.	4	1	4				
Safeguarding concern disclosed through messaging and not reported/followed up	A vulnerable person discloses harm via direct message and this is not reported	Must follow safeguarding procedures – inform the Parish Safeguarding Officer that day. Do not delete any such messages. Do not attempt to resolve anything yourself.	3	1	3				

Key: Sev. = Severity, Prob. = Probability

Issue/how harm can occur	Example	Current/existing control measures	Risk rating based on existing controls			IMPROVEMENT PROGRAM			
			Sev.	Prob.	Risk	Additional control measures	RESIDUAL RISK		
							Sev.	Prob.	Risk
		<p>Inform the police using 999 if someone is at immediate risk of harm.</p> <p>Disclaimer on social media accounts that they are not monitored all the time so an immediate response will not be given</p>							
Loss of account access	Volunteer who managed the account leaves and credentials are lost	All account login details to be shared with Social Media Co-Ordinator.	2	1	2				
Use of church account for personal or political views	Admin posts personal views on immigration	<p>All external posts should relate to church activities and not include personal or political views.</p> <p>Account administrators are known to the Social Media Co-Ordinator and receive guidance about what is/is not appropriate.</p> <p>The Social Media Co-Ordinator has access to accounts and can delete posts.</p>	3	1	3	It may be appropriate to post an apology			
Harassment or abusive behaviour on church page/account	Commenter targets individuals or groups	<p>Settings for comments to be configured so that, if they are not necessary, they are disabled.</p> <p>Comments may be locked for a post if needed.</p> <p>Social Media Co-Ordinator can be contacted to advise on moderation if required.</p>	3	1	3				
Unsolicited and inappropriate messages from children or vulnerable adults	Child direct messages the church Instagram account and shares indecent images of themselves	<p>Disclaimer on social media accounts that they are not monitored all the time so an immediate response will not be given.</p> <p>Any offensive images received should not be downloaded, copies made or forwarded as this is an offence.</p> <p>Do not forward it to anyone</p> <p>Preserve the message evidence within the platform</p> <p>Record:</p> <ul style="list-style-type: none"> - date and time the message was received - the social media platform - username/account involved 	4	1	4				

Key: Sev. = Severity, Prob. = Probability

Issue/how harm can occur	Example	Current/existing control measures	Risk rating based on existing controls			IMPROVEMENT PROGRAM			
			Sev.	Prob.	Risk	Additional control measures	RESIDUAL RISK		
							Sev.	Prob.	Risk
		<p>- who had access to the account at the time Report immediately to the safeguarding officer.</p> <p>Do not ask questions about the image or the situation.</p>							
Unmoderated messaging with children or vulnerable adults	Administrator misuses account to groom a child via direct messages	<p>Account administrators are known to the Social Media Co-Ordinator and receive guidance about what is/is not appropriate: Any messaging should be brief and limited, and focussed on engagement with face-to-face church activities.</p> <p>Social Media Co-Ordinator has access to all church accounts and periodically checks direct message logs.</p> <p>Anyone suspected of such behaviour to be reported immediately to the Safeguarding Officer. Login details to be changed by the Social Media Co-Ordinator immediately and not shared with the suspected person. All messages to be kept on the platform as evidence.</p>	5	1	5				

Key: Sev. = Severity, Prob. = Probability