St John's Church Harpenden
Social Media+ policy

Policy Owner	Com Committee
Last updated	Nov 2020
Last adopted by PCC resolution	Nov 2020

Introduction

Social media is now a mainstream method of communication, especially amongst younger people. The term is both broad and narrow. It includes dedicated sites, apps, Skype, blogs, emails, messaging, texting (these last three are not strictly social media but need similar safeguards); this list is not exhaustive. Web-based communication tools enable people to interact by sharing and receiving information in many forms. It is primarily a public means of communication rather than a private one.

Most social media platforms will have features such as the following:

- User accounts – so you can log in and take part.
- Profile pages – to give information about you, the user.
- Friends, groups, followers – people who have connected with you.
- News feeds – information from people you choose to connect with.
- Posts – items you write, photograph, record or video and place on the site.
- Comment – the chance to write a response or click a 'Like' button on someone's post.

The following policy statement seeks to lay down parameters for its use within St John's Church organisation.

Policy

The following guidelines cover all types of social media platforms such as Facebook, Twitter, Instagram, YouTube, etc. but also extend to the use of mobile phones (including texts), blogs, website forums and emails. They should be read in the context of St John's Safeguarding, and Data Protection (GDPR), policies.

- All St John's Official Social Media accounts must be linked to a St John's Church email address.

- The maintenance of records and posts, wherever possible, is key to good practice.

- Content issued by the church must be appropriate, clear, and take lower age limits into account. It must be managed, as well as responses to ensure acceptable behaviour, and language. Special protections are to be taken for the under 18s, and the under 13s, in accordance with government guidelines. For example, parental permission is required for these two categories.

- Offensive, bullying, abusive, sexually inappropriate, libellous, defamatory, or illegal content are risks that can be mitigated by close and regular monitoring. Content that breaches copyright or data protection, or seeks to unduly influence, or cause harm or potential harm, should be dealt with, and reported to the appropriate agencies if necessary.

- It must be made clear that postings on the internet are permanent and public.

Responsibilities of all church members (especially leaders of groups and activities)

1. To use social media well as servants of Jesus Christ, communicating with integrity and accuracy. Each leader is a role model for their church and the Christian faith.

2. To always express all messages in an appropriate tone: friendly, polite, courteous and never rude, abrupt or over-familiar. Avoid hasty, ill-thought out responses to blogs, tweets, etc.

3. To ensure that the 'professional', i.e. the role in which one is communicating, is kept separate from the personal.

4. To be aware of, and minimise, the risk of messages being taken as official church policy, by means of appropriate disclaimers.

5. To ensure that no-one's private or family information and contact details, are disclosed on a public platform.

6. To conserve and file records of official church messages so that they are able to be traced at a later date.

7. On live calls, to be aware of what may be seen on a webcam, both foreground and background.

8. To not hide your identity or use an alias.

Additional guidelines for working with young people or vulnerable adults

1. Do not communicate via social media or mobile phones, with children in Year 6 or below, other than within one's immediate family. The following statements are designed for those working with young people in Years 7 to 13 and assumes an official church account will be used.

2. To exercise appropriate discretion but never to promise total confidentiality in any mobile or internet-based communication.

3. To not contact any young person by means listed here just before or during normal school hours or after 9.00 pm.

4. To inform young people that no leader is under any obligation to respond to any communication immediately and especially if they are at work, at family events or, for church staff, on their day off.

5. Where possible, to hold conversations with young people face-to-face rather than by email, text or phone. Contact by these means should be related to church work and not used for private conversations or socialising. Where social media are used, screen-shots or copies of conversations should be kept for future reference.

6. To only provide contact details that are within the public domain.

7. To immediately inform the church's Safeguarding Officer should any communication by any means listed here raise safeguarding issues.

8. To understand that this policy is overseen by the Communications Committee and the PCC who are authorised by the Trustees to ensure that all church workers comply with it, and who have authority to monitor the use of whatever electronic media, linked to St John's named accounts, are used for communication within the church. Leaders are asked to agree to such monitoring on their appointment. Although we hold this authority to monitor, in practice there has to be trust that electronic media is being used for the correct purposes and safely, unless there is a safeguarding issue or any other breach of trust.

9. To ensure that team leaders are kept aware of the types of communication being used by leaders within their team, and to immediately report to the team leader any inappropriate material received.

10. To ensure that leaders word their personal profiles in a responsible way, knowing that these will be accessed by young people and their parents who will see the leaders as role models for the church and the Christian faith.

11. Not to 'like' or comment on inappropriate or offensive items or photographs.

Parental permission for young people

1. Parents and guardians will first be asked to consent to young people having contact with leaders by means of email, texts and mobile calls according to this policy.

2. They will also be asked to give consent to their child connecting to their group's Facebook page.

3. They will also be asked to give consent to the use of photographs of their child as authorised by the church appearing in church publications, the church website, a Facebook group and displays provided such adhere to the church's policy on the use of children and young people in photographs. See Safe Use of Images Policy.

4. Parents will be informed of the type of electronic communication being used in their child's group and asked to confirm their agreement on these issues on an annual basis.

Use of particular social media with young people:

Facebook

1. No leader should, without formal authorisation, be friends with an under-18-year-old with whom they work or for whom they are responsible within their leadership role.

2. There should be no hidden communication through private messaging or use of any leader's personal social media account. Only allow friends to post on your timeline.

3. Facebook groups set up with due authorisation by the church must strictly adhere to the church policy for groups which should include the following.
   - All groups should be closed, for over 13's only, and set up with a secure profile.
   - Each group should be monitored by two church adults who have been authorised by the Trustees. They should have admin rights.
   - Photographs of events and people of all ages may be posted but only once authorised by the group's monitors and with privacy settings set so that only group members can see them, unless there are signed permissions.

Twitter & Instagram

1. No leader should, without formal authorisation, follow an under-18-year-old with whom they work or for whom they are responsible within their leadership role, although young people may follow adults. There should be no hidden communication with young people through direct messaging (DM)note to point 2 under Facebook above.)

2. Leaders who tweet/instagram must be aware that their tweets/instagrams may be monitored as above.

Other

1. No church adults should connect with young people on Snapchat.

2. No church adults should subscribe to any young person's YouTube channel.

Skype and young people

1. Use of Skype for one-to-one communication with young people is not permitted.

2. It is permissible to use it for conference calls or group messages when first authorised by a team leader or monitor.

3. Wherever possible Skype calls should be made to a family computer in a main living area and not to a private computer in a young person's bedroom.

Emails to young people

1. Always ensure a team leader (not your spouse) is copied into any message to a young person and do not use the bcc line. Do not use email to recruit to the group.

2. Emails sent and received should be via an official church address and kept on file for an agreed length of time so that they cannot be hidden and can be checked. For leaders with no access to a church address, all emails should be copied to a team leader who does have one.

3. Leaders may hold email addresses of young people in a personal address book but only whilst they remain an authorised leader of a church group or activity.

4. No member of church staff may use private email accounts for any communication with church young people but only church accounts kept on a central server.

Texting and mobile use with young people

1. Authorised leaders may communicate with young people by text or phone call within the guidelines given above. If texting is required then the authorised leader should have an official phone provided by the PCC for this purpose, which is separate from their personal mobile phone.

2. Text communication should be kept brief and factual (e.g. the date of a meeting) rather than providing comment or holding a discussion.

3. Leaders may hold young people's contact details in their phone's memory but only data already in the public domain. All such details should be immediately deleted once the leader steps down from office or the young person leaves the group.

4. No leader should ever send an inappropriate image of themselves to a young person.

5. The aim should be to save messages in text files to ensure an open record exists.

Relevant links that have contributed to the formulation of this policy:

https://www.gov.uk/government/publications/child-safety-online-a-practical-guide-for-providers-of-social-media-and-interactive-services/child-safety-online-a-practical-guide-for-providers-of-social-media-and-interactive-services

CEOP: www.ceop.police.uk/safety-centre

IWF: www.iwf.org.uk