Acceptable Use Policy for Wi Fi, Mobile Phones and Social Media

This policy is written in line with the National Safeguarding Standards to foster and promote a safe and healthy culture for all. Also refer to the Safeguarding and GDPR policies together with the Safer Working Practice Protocol for Working with Children and Youth. Minors are defined in this policy as children and young people under the age of 18 years.

St Thomas a Becket Church provides employees, and others, with access to the internet with the intention of increasing productivity and enhancing church-related communication. While this access has the potential for employees to do their jobs faster or smarter, there is justifiable concern that is can also be misused. Such misuse can waste time, potentially violate laws, other St Thomas a Becket policies, garner negative publicity for the church and potentially expose it to significant legal liabilities. This policy, which applies to all within the church, is designed to facilitate understanding of the expectations for the use of these resources.

Use of the church Wi Fi

- The church reserves the right, and will take reasonable steps, to block any site that it deems inappropriate. However, there is no guarantee that all inappropriate content will be blocked.
- Access to the church WiFi is password protected and should only be shared with responsible adults who need legitimate access.
- The Church reserves the right to terminate an Internet session that disrupts church services or that involves user behaviour that violates The Church's policies.
- As with all church resources, we affirm that it is the responsibility of parents/guardians, NOT church staff, to determine and monitor their minor's responsible use of the Internet when in church
- Since software and information downloaded from any sources, including the Internet, may contain computer viruses, users are advised to utilise virus-checking software on their computers.
- The Church is not responsible for damage to users' equipment, nor for any loss of data, damage or liability that may occur whilst using The Church's wireless network, or Internet connections.
- Church staff will not monitor a user's Internet history but as this will be directly traceable to St Thomas a Becket. Users must immediately close and certainly not visit sites which:
 - Are illegal under current law.
 - Are defamatory, threatening or intimidatory or which could be classed as harassment.
 - Contain obscene, profane or abusive language.
 - Contain pornographic material whether in writing, pictures, films or video clips.
 - Contain offensive material regarding any of the legally protected characteristics.
 - Infringe third party rights or are otherwise unlawful.
 - Promote violence.
 - Infringe copyright.
 - Users should not attempt to gain access to restricted areas of the network or to any
 password protected information without being duly authorised to do so.





Mobile Phones and Social Media

Social media is immediate, interactive, conversational and open-ended. This sets it apart from other forms of communication and demands a new way of thinking. As well as the many opportunities, users should also be aware of (though not put off by) the associated risks. St Thomas a Becket church makes use of social media sites to share content and keep in touch with the community and worshippers. Written permission will be sought for the inclusion on any of the church's social media sites. Remember, if you would not say this to someone's face DO NOT put it on-line. All workers using church phones are accountable to the incumbent who will monitor communications as necessary.

All users need to adhere to the following:

1. Don't rush in

The immediacy of social media is one of its benefits – users can respond quickly to questions, correct misunderstandings, give their perspective about a breaking story in the news media. Responding quickly doesn't mean doing so without due consideration.

Before posting consider:

- Is this my story to share?
- Could this be 'Fake News'?
- Would I want my mum to read this?
- Would I want God to read this?
- Would I want this on the front page of a newspaper?
- The tone of a particular forum, if and how you might participate.

2. Transient yet permanent

Social media updates are immediate and will outdate quickly BUT they can have a more lasting impact and users should assume that anything they post is permanent. Even if it is deleted later, it may have been seen and re-published or referred to elsewhere.

3. Be an ambassador

If a user is employed by the Church or a member of the Church, others will see them as a representative of the Church: So, their actions matter.

- When talking about church matters, users must make it clear whether these are personal opinions or those of the Church of England /Diocese.
- Use clear, appropriate and unambiguous language in all communications
- Log off promptly so that nobody else can pretend to be you

4. Don't hide

When the account is a shared one, for example, a Facebook page for the church, ensure people can easily find out who is responsible for the content. Anonymity and 'hiding' behind aliases when using social media is not acceptable and it is at odds with the church ethos.

5. Blurring of public/private life boundaries





In everyday ministry, the distinction between public duties and private life is difficult to draw. It is no different online. There are risks associated with personal opinions being seen as public statements, a minister's private life being invaded and the difficulties of detaching from work. Employees must, as far as possible, have different accounts for ministry and personal use to help set definite boundaries and use privacy settings wisely.

6. Safeguarding (see separate policy also)

The informality that social media encourages can mean that it might be harder to maintain a professional distance that is required when working with children, young people and the vulnerable.

- DO NOT add children, young people or vulnerable adults, who you have met through church activities, as friends to personal accounts.
- Personal and Church social media and email accounts must be kept separate, as far as possible.
- Communicating directly online with someone, for example with private messaging, is like
 meeting them in private. You're advised to send messages to groups, rather than individuals,
 or to share them publicly.
 - A list of all Church social media groups is to be kept up to date and any new groups created must be added to this list. Only group leaders should be allowed admin rights and there should be at least two admins for any WhatsApp or Messenger group.
 - Group admins should monitor messages to ensure appropriate use of the group. Any
 offensive or defamatory messages should be deleted and reported to the Safeguarding
 Officer, and the person sending such messages removed from the group.
 - If group users start to contact you directly, please advise them that messages need to be sent through the group or to work contact details only (work email or work mobile). Any response will only happen during normal working hours.
- Be on your guard about fake friend requests and phishing scams.

7. Photography

Sharing photos online is a good way to promote our church and what we do.

- However, you must make sure you have permission from anybody who features in the image before sharing, storing or publishing.
- Written parental permission is needed before any children are included in photos: avoid the use of names or anything else that could identify the children.
- Be ready to remove an image as quickly as possible if requested.
- Photographs taken during events by church members, which are for church publicity, must be sent to the church administrator to check that permission has been granted
- Avoid taking photographs during services. If photographs are to be taken during a service, this should be pre-arranged with the service leader, who should announce that photographs are being taken discreetly and only of those who have granted permission, so as not to distract others from worship.

Baptisms and Weddings can present particular, but different, challenges.





- In both cases the minister must make it clear what is, and what is not, acceptable during the service. St Thomas a Becket clergy will agree the main points that must be made and have this available for everyone to use.
- Documentation for baptism preparation will make it clear that there should only be one nominated photographer during the service and that only members of the baptism party should be included in any photos.
- Weddings usually have an official photographer(s). The minister should check with the
 couple whether to ask the wedding guests not to post on social media before the bride and
 groom have done so.

8. Stay within the legal framework

Whilst sharing thoughts and reflections with friends or followers via social media can seem personal and private, it is not. By law, if one or more people can access it, content is classed as published, in the public domain and subject to legislation around libel, defamation, copyright and data protection. Please do not

- transmit harassing, illegal or offensive material
- infringe copyright
- engage in defamation of character
- disclose any confidential or personal information

9. Confidentiality

Use of social media does not change the Church's understanding of confidentiality. Within the life of the Church there are private meetings and conversations, particularly in terms of pastoral work. A broken confidence via social media could spread rapidly and be impossible to retract.

10. Be mindful of your own security

- Don't overshare personal information.
- Never publish detailed personal information e.g. address or telephone number, unless in a private message to someone known and trusted.
- Don't assume anything online is confidential or secure

This policy was agreed by PCC on

Review will be annually

Signed by:

Chair of PCC

