Stranton All Saints and Burbank Community Church: Information Technology Communications and Social Media Policy

1. Why do we need a policy?

Information Technology Communications and Social Media ("IT & SM") are an increasingly important means of Clergy, Paid Staff, Volunteers and Church members communicating within the Church family, with other Churches, and to the wider community. For Stranton Church, the term "Social Media" includes use of electronic communications for a wide variety of potential purposes, ranging from proclaiming the Kingdom in broadcast video and graphical content and publication of information, to private (person to person and person to group) messaging with text and video content and links to other Social Media. As well as being an enabler for powerful and easily accessible personal and group communication, the use of IT & SM carries high risks for potential misuse. Abuses of IT & SM (such as "trolling", "ghosting", misleading and inaccurate "posts", and distribution of unauthorised personal information) by individuals within the Church and from outside can be very damaging both to individuals and to the reputation of the Church. A policy is therefore needed to guard against adverse consequences for individuals and the Church arising from inappropriate or malicious use of Social Media.

2. Scope and Applicability

This policy covers the varied uses of IT & SM applications by Clergy, Paid Staff, Volunteers and Church members, such as providing virtual spaces for meetings, teaching and social interaction, for live streaming of worship services , and support for business (PCC and Clergy) meetings. It includes virtually all methods (other than traditional 1:1 voice telephony) for personal and public contact by electronic means using mobile data, messaging via telephone, email and internet on a variety of technical "platforms" (including smartphones, smartwatches, virtual reality headsets, tablet and other internet enabled devices, laptops, notebooks, and desktop computers) equipped for one or more of voice, text, video and data communications.

As IT & SM are evolving rapidly and continue to develop additional functionality and capability, it is not possible to define an all embracing set of specific rules for their use covering all eventualities: this policy therefore sets a framework for safe use and effective oversight by the PCC of IT & SM by Church members and leaders, for all circumstances where the Church offers either open or restricted access to IT & SM accounts - for example but not limited to, WhatsApp Groups, Facebook pages, Website content and" Zoom" meetings - providing content and/or virtual meeting space and personal messaging for use by Clergy, Paid Staff, Volunteers and Church members, an "IT & SM account" includes any technological platform or resource **published or made available by or in the name of Stranton Church, Burbank Community Church or the Central Hartlepool Group of Churches** for clergy, paid staff, volunteers and Church members to interact with each other, parishioners, visitors, or the wider public.

The PCC cannot regulate the private use of IT & SM by Church members on their own account , but if it or the Safeguarding officer becomes aware of an individual in a position of perceived authority (as a leader or member of staff in the Church) using personal IT & SM in apparent contravention of Church policy on Safeguarding or Data Protection , the applicability of those policies (below) should be considered.

Personal IT & SM accounts of clergy, paid staff and IT & SM administrators should not be used for official Church business or in a manner that could be construed as holding out use as sanctioned by the Church, unless that is actually the case e.g. clergy or officers' personal email accounts. In addition to providing clarity for users the fundamental reason for this is that uncontrolled "free to use" apps may not include the level of security and encryption as apps which have been risk assessed as part of the PCC evaluation and approval process, and for which a subscription licensed version may provide more effective security against hacking and malware intrusion.

3. Over-riding and related policies:

The following policies are relevant to the use of IT & SM and must be applied as necessary in the interpretation and application of this policy:

- Safeguarding Policy
- GDPR Data Protection Policy
- Health and Safety Policy
- Use of Information Technology Equipment and Services

4. Policy context – the Current Church of England Guidelines and Code of Conduct

This IT & SM Policy is set in the context of current national guidelines of the Church of England:

https://www.churchofengland.org/terms-and-conditions/our-social-media-community-guidelines

By engaging with the Stranton and Burbank, Central Hartlepool Group, the Church of England and Archbishops' IT & SM accounts, Church members, workers and clergy agree to abide by the following nationally agreed community Guidelines, which amount to a code of conduct for users:

- **Be safe**. The safety of children, young people and vulnerable adults must be maintained. If you have any concerns, contact the church Safeguarding officer on one of the contacts signposted in the Church Safeguarding policy.
- **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, remembering that tone often does not translate well via Social Media.
- **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 in public posts as well as private online meetings can be places of robust disagreement and it's important we apply our values in the way we express them.
- **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 re-posting or amplifying: the Internet is an environment where falsehoods and misrepresentation can obscure truth.

- **Follow the rules**. Abide by the terms and conditions of the various IT & SM platforms themselves. If you see a comment that you believe breaks their policies, then please report it to the respective company.

In accordance with these Guidelines, in the adoption of this policy Stranton Church formally undertakes to be a Church Signatory to the Digital Charter of the Church of England and encourages its Clergy, Staff and Volunteers to become personal signatories to the Digital Charter

https://www.churchofengland.org/terms-and-conditions/our-digital-charter

5. Statement of Policy

Stranton Parochial Church Council will have oversight of the use of all IT & SM applications used on behalf of, provided by, or in the name of Stranton and Burbank Community Church by clergy, paid staff, volunteers and Church members employed or engaged on behalf of Hartlepool Central Group of Churches, whether they are intended for use by individuals or groups.

The PCC will formally approve the use of each instance of particular proprietary IT & SM platforms in the name of the Church or by the Central Hartlepool Group, whether for public audiences or closed groups such as staff meetings, cell or house group meetings, young persons' groups or Bible study/teaching with specific groups, which must be subject to configuration and supervision controls implemented by at least one named administrator in each instance (e.g. each Facebook page).

Named Administrators for each instance of IT & SM must be approved and acknowledged by the PCC to act on behalf of the Church.

The PCC will issue application-specific technical and user guidelines for the safe, secure, and acceptable use of IT & SM, in accordance with the Church of England digital charter which is to be adopted by the PCC and by individual Staff and volunteers who are involved .

IT & SM cannot replace or be a substitute for other more traditional interpersonal contacts. There is a risk of disenfranchisement of individuals who for various reasons (including age, access to resources, learning difficulties, and adverse previous experience with information technology) cannot or choose not to engage with Social Media. In developing IT & SM as part of any communications strategy for the future development of ministry and mission the Church will also provide assistance to individuals to help overcome barriers to access, and continue to provide alternative channels of paper and contact based communication.

6. Configuration controls for configurable IT & SM applications must include:

Where an application permits 1:1 online chat or person to person messaging in a manner that is concealable from other users, and that application is to be used by a group that includes young people or vulnerable adults) the policy is to ensure that, either by configuration settings or using agreed written procedures, such functionality is not used by any individual in a position of authority to message individuals privately (examples of configurable applications include Facebook and Zoom).

Security of access to virtual meetings will be arranged to prevent malicious hijacking or security breach including confidential use of passwords, host controls such as waiting room admission and lockdown, and pre-registration of users who are leaders.

For complex configurable IT & SM applications, a training needs assessment will be undertaken and in house and/or external training provided if/as required to administrators and/or users , which may consist of or include proprietary or public access materials.

The introduction of a new or upgraded IT & SM application in to Church use will be subject to a configuration and use risk assessment performed or commissioned by the PCC Standing Committee or other delegated subcommittee, including as appropriate, the Communities of Hope Project Steering Committee. Risk assessments will be shared with the Safeguarding Officer of the PCC and where applicable the PSOs for the Central Hartlepool Group of Parishes.

A review and risk assessment of IT & SM applications already in use at the time of approval of this policy will be undertaken to identify and mitigate any configuration risks and issues identified, having regard to this policy.

7. Supervision controls for each approved IT & SM application must include:

- Approval by the PCC of IT & SM Administrators (at least one administrator for each instance in use) to take responsibility for reviewing content, the deletion or removal of out of date inaccurate misleading abusive or hostile material or inappropriate material/posts, giving guidance to users in accordance with this policy for safe use. The administrators should be subject to DBS checks appropriate to the target audience of the IT & SM and have received relevant training in Safeguarding and Data protection.
- Regular (at least monthly) review and housekeeping of "posts" and information updates, by the approved named administrators - if necessary blocking individuals who make repeated inappropriate contributions.
- Identifying individuals who repeatedly misuse the Church IT & SM (such incidents being reportable under the Safeguarding and Health and Safety Policies (or GDPR).
- GDPR protection of and management of explicit consent for disclosure of personal identifiable data in IT & SM by anyone other than the data subject. For example, do not pass on an email address or telephone number belonging to someone else without their approval) .
- Maintenance and observance of any safeguards, policies, conditions of use, specific codes of conduct for users and controls recommended or directed by the IT & SM service providers.
- Observance of copyright law in streaming third party material (only within the licensing permitted, and with inadvertent breaches rectified immediately)

Recording, broadcast and re-publication of video or audio content will be subject to all users affected giving prior consent.

8. IT & SM platforms used in communicating with young people <18 years.

Specific measures must be in place to ensure and enhance protection for young people involved in Church groups' IT & SM (particularly messaging and video) applications:

Express consent must be in place from a parent or carer for a young person to participate in any Church IT & SM group. Written consent from parents/carers must be obtained in order to a) use and store photographs of children/young people on the church's social media and website, b) use telephone, text message, email and other messaging services to communicate with young people, c) allow young people to connect to the Church's social media pages, d) meet with young people on any video conferencing platform.

Rules for participation must include “open door” communication where individual young persons are not permitted to participate from bedrooms or private spaces. Young people will be made aware that any communication will be viewed by all users. Any messages and threads through social networking sites will be saved (i.e. as hard copy or “screen shots” prior to deletion if content breaches this policy) so that evidence can be provided, if required, of the exchange. One-to-one communication with children and young people must be avoided. Visual media must not be used for one-to-one video conversations with young people either in Church IT & SM channels or by Church officers on own personal social media accounts.

Clear and unambiguous language must be used in all communications, avoiding abbreviations, in order to minimise the risk of misinterpretation or covert misuse.

Any inappropriate material received posted or displayed through social networking sites of other electronic means must be saved and downloaded to hard copy and shown without delay to the PSO, incumbent or, if appropriate, DSA.

The named administrators for young persons’ groups are bound by professional rules of confidentiality: but where there is a concern that a young person or adult is at risk of abuse, or they themselves pose a risk of abuse to others, safeguarding procedures must always be followed. Clear boundaries must be made between personal SM usage and that for public ministry; Church account(s) and profiles must be separate from personal accounts. Personal accounts must not be used in work with children, young people or vulnerable adults. Children, young people and vulnerable adults must not be added as “friends” on personal accounts. In addition, personal accounts should have a high level of security so they cannot be accessed by those who are not listed as “friends”

9. Video Conferencing with Children and Young People

It may, at times, be appropriate to use video conferencing to meet with a group of children or young people or hold an online service. “One to one” video calling by a Church leader to a young person is not permitted. In video conferencing, these additional points apply:

- Written prior parental consent must be obtained. This may be electronic, e.g. by email.
- Meeting invitations and joining details will be emailed to parents/carers, rather than to the young people themselves.
- A parent/carer is required to be present at all times during the session, making themselves
- known at the beginning and end of the session and being around in the background at all times.
- At least two people who have been safely recruited to work with children / young people should be present in a video conference. These should both be “live” in the meeting before children or young people can join the meeting.
- All participants should be in a communal area of their home (not in bedrooms or bathrooms).
- All participants should be fully dressed in daytime clothes.
- Video conferencing will not be recorded for later playback or broadcast as live stream unless all parents/carers have given prior express consent. E.g. for a youth service online

10 Types of IT & SM not approved for Church use

Certain forms of IT & SM are not amenable to oversight and review, as they are only or mainly used for sending transient encrypted messages to individuals. An example is “Snapchat”, a “one to one “photo messaging” app, in which messages are usually only available for a short time before they

become inaccessible to their recipients. Use of such applications by Church Groups is not recommended or locally approved for official use because of the risks associated with undetectable inappropriate use. For this reason some functions of otherwise acceptable IT & SM should be generally (or particularly, in the case of young people) avoided, such as video calling in "Whatsapp"

11 Flexibility of response

It is sometimes necessary for a new IT & SM application or instance to be set up for a specific reason at short notice: the Chair of the PCC must be notified if this is the case, with assurance of compliance with this policy to be ratified at the next Standing Committee or PCC meeting.

12 How will we respond to people who breach the Church's IT & SM policy and community guidelines?

The Church's and Archbishops' National Communications teams may take action if they receive complaints or spot inappropriate, unsuitable or offensive material posted to the Church national IT & SM accounts.

Stranton PCC will through its IT & SM Administrators include all necessary measures for local oversight and management including advice to users where necessary in the acceptable use of IT & SM (in cases where the guidelines of the Church of England are not being followed) deleting inappropriate posts content and comments, blocking users who persistently breach policy or guidelines, and will notify the PSO and relevant authorities in the event of any safeguarding or health and safety incident or concern, or a reportable breach of GDPR.

13 Review:

This policy is to be reviewed not more than three months from date of implementation (appointment of administrators) and annually thereafter.