

Social Media Policy

St Peter's, Colchester

Adopted by the PCC: [tbc]

Review date: [annually]

Policy owner: The Parochial Church Council

1. Purpose

This policy explains how social media, messaging platforms, livestreaming and online communication should be used by those who serve, lead, work, govern, volunteer or act on behalf of St Peter's.

Social media can help St Peter's share the gospel, welcome newcomers, promote church activities, encourage the church family, and communicate quickly and effectively. It can also create risks, including safeguarding concerns, loss of confidentiality, misuse of personal information, reputational damage, bullying, harassment, misunderstanding, inappropriate boundaries, and confusion about who is speaking on behalf of the church.

The Parochial Church Council has responsibility for the governance and oversight of St Peter's. As disciples of Jesus Christ, we seek to be faithful in all that we say and do, including how we communicate online. This policy is intended to help our online communication be truthful, gracious, safe, lawful, pastorally wise, and consistent with the Christian witness and responsibilities of St Peter's.

2. Scope

This policy applies, as relevant, to:

- clergy, licensed and authorised ministers;
- employed staff;
- PCC members;
- churchwardens and other elected or appointed officers;
- ministry leaders;
- volunteers;
- those managing or contributing to St Peter's official social media, website, livestreams, WhatsApp groups, email lists or other online communication channels.

It applies to official St Peter's communications and, where relevant, to personal online activity that could reasonably be associated with St Peter's or affect the church, its members, staff, volunteers, children, young people, vulnerable adults, hirers, partners or reputation.

Social media and online communication include, but are not limited to:

- Facebook;
- Instagram;
- X / Twitter;
- YouTube;
- TikTok;
- WhatsApp;
- livestreaming;
- blogs;
- websites;
- email lists;
- messaging apps;
- online forums;
- similar platforms or services.

3. Christian foundation

Christian communication should be marked by truth, grace, wisdom, self-control and love for neighbour.

The Apostle Paul writes:

*“Let your speech always be gracious, seasoned with salt,
so that you may know how you ought to answer each person.”*
– Colossians 4:6, ESV

Those who communicate online in connection with St Peter’s should therefore seek to speak truthfully, kindly, carefully and constructively. Online communication should never be used for gossip, bullying, harassment, manipulation, contempt, factional behaviour, personal attack, discrimination or misuse of power.

Most simply, we should seek to treat others online as we would wish to be treated ourselves.

4. Official St Peter’s social media and online channels

Official St Peter’s accounts, pages, groups, websites, livestreams and online communication channels must be authorised by the Vicar, Church Administrator, PCC or another person delegated to oversee communications.

Official accounts should normally:

- have at least two authorised administrators or account holders;
- use church-approved contact details where practical;
- have secure passwords and appropriate access controls;
- be used only for proper church purposes;
- be monitored and moderated appropriately;

- avoid unnecessary personal information;
- follow St Peter's safeguarding, data protection, copyright and communications requirements.

Access to official accounts must be removed promptly when a person no longer needs it for their role.

Posts on official channels should be accurate, gracious, pastorally wise and consistent with St Peter's Christian ethos and policies. They should not imply PCC approval for matters that have not been approved.

Official St Peter's channels must not be used for party-political campaigning or to imply that St Peter's endorses a political party or candidate.

St Peter's will keep under review whether any official online channel, group, forum, messaging service or other digital service creates additional legal responsibilities under the Online Safety Act 2023 or other online-safety legislation. Where such responsibilities apply, St Peter's will take appropriate steps to comply, including through moderation, access controls, reporting arrangements, safeguarding procedures and, where necessary, advice from the diocese, Charity Commission guidance or other appropriate sources.

5. Personal social media use

Those who serve, lead, work, govern, volunteer or act on behalf of St Peter's should take care that their personal online activity does not undermine the church's witness, damage trust, breach confidentiality, compromise safeguarding, or create confusion about whether they are speaking for St Peter's.

Personal social media accounts should not normally use church email addresses, church branding or church resources unless this has been authorised.

Those covered by this policy should not use personal online platforms to:

- attack, abuse, bully, harass or intimidate others;
- make defamatory, malicious or knowingly misleading comments;
- disclose confidential church, pastoral, safeguarding, staff, volunteer, PCC or personal information;
- share contact details, images or videos of others without permission or another lawful basis;
- post material that is sexually inappropriate, exploitative, abusive, hateful or unlawful;
- post discriminatory or derogatory material relating to age, disability, gender reassignment, marriage or civil partnership, pregnancy or maternity, race, religion or belief, sex, sexual orientation, or any other inappropriate distinction;
- bring St Peter's into disrepute;
- use their role, influence or access at St Peter's for improper personal advantage.

If a person can be identified as connected with St Peter's, they should take particular care that their online conduct is consistent with the trust placed in them.

Personal political opinions may be expressed in a personal capacity, but church channels, church resources, staff communication systems and official St Peter's accounts must not be used for party-political campaigning.

If someone from the press or media contacts a member of staff, PCC member, volunteer or ministry leader about online content relating to St Peter's, they should not respond on behalf of the church unless authorised to do so. They should refer the matter to the Vicar, Churchwardens or Church Administrator.

6. Safeguarding and online contact

Safeguarding is central to the life of St Peter's. Online communication must follow St Peter's Safeguarding Policy, Church of England safeguarding guidance, diocesan guidance and any role-specific safeguarding requirements.

Adults acting on behalf of St Peter's must not use personal social media accounts to form private online relationships with children or young people connected with church activities.

Where online communication with children or young people is necessary for a church role, it should normally:

- use an approved church or ministry channel;
- have parental or carer awareness and consent where required;
- be visible and accountable, with more than one authorised adult able to see the communication;
- be limited to proper church purposes;
- avoid one-to-one private messaging where possible;
- take place at appropriate times;
- avoid disappearing-message platforms or settings where records cannot be kept;
- be consistent with the relevant Ministry Role Description and safeguarding arrangements.

Any safeguarding concern, disclosure or worrying online behaviour must be recorded and reported through St Peter's safeguarding procedures. It must not be handled merely as an ordinary complaint, private disagreement or informal pastoral matter.

No one should promise absolute confidentiality where there is a safeguarding concern, risk of harm, abuse, coercion, criminal behaviour, or danger to a child, young person or vulnerable adult.

7. Photographs, videos, livestreaming and consent

Images, videos and livestreams can help communicate the life of the church, but they must be used carefully.

St Peter's will seek appropriate consent before using identifiable images or videos of individuals, especially children, young people and vulnerable adults. Consent arrangements should be clear about how images may be used, including website, social media, printed publicity, livestreams or displays.

When using images of children or young people, those acting for St Peter's should:

- follow safeguarding and data protection requirements;
- obtain parent or carer consent where required;
- avoid unnecessary identifying details, such as full names, addresses, schools or contact details;
- avoid images that could embarrass, exploit or place a child or young person at risk;
- use official church channels rather than personal accounts;
- remove images where consent is withdrawn or a safeguarding concern arises, where reasonably possible.

Livestreaming and photography at services or events should be managed with clear notices, appropriate camera angles, and reasonable provision for those who do not wish to be filmed or photographed.

8. WhatsApp groups and messaging

WhatsApp and similar messaging platforms may be useful for rotas, church groups and ministry communication, but they must be used responsibly.

Church-related WhatsApp groups should normally:

- have a clear purpose;
- have appropriate administrators;
- be limited to current St Peter's members, participants, parents, carers, staff, volunteers or others who genuinely need to be included for the purpose of the group;
- be consistent with ChurchSuite records where relevant;
- be reviewed periodically by group administrators;
- have members removed when they no longer need access.

Group administrators may remove content, restrict posting, close discussion, change group settings, or remove members where necessary.

This includes removing or restricting members whose identity or connection with St Peter's cannot reasonably be confirmed, who no longer need access to the group, or who post inappropriate, disruptive, unsafe, confidential, abusive, misleading, unlawful or otherwise unsuitable content.

Where appropriate, administrators may also report content or users to the platform, preserve relevant records, refer concerns to the Vicar, Churchwardens, Church Administrator, Parish Safeguarding Officer or PCC, and seek diocesan, legal, safeguarding or police advice.

Participants should:

- keep messages relevant to the purpose of the group;
- communicate with courtesy and restraint;
- avoid gossip, argument, pressure, factional behaviour or inappropriate humour;
- avoid sharing confidential, pastoral, safeguarding or personal information;
- avoid forwarding messages, images or contact details outside the group without permission;
- double-check recipients before sending sensitive or potentially personal information;
- report safeguarding or serious conduct concerns through the proper channels.

WhatsApp groups involving children or young people require particular safeguarding care and should only be used in accordance with approved safeguarding arrangements.

9. Confidentiality, data protection and security

Those using social media or online communication for church purposes must follow St Peter's Data Protection Policy, Privacy Notice, Data Retention Policy, IT Security Policy and IT Acceptable Use Policy, where applicable.

They should:

- use personal data only for proper church purposes;
- avoid sharing contact details without permission or another lawful basis;
- protect passwords and login details;
- use strong passwords and appropriate security settings;
- avoid using shared or insecure devices for confidential church work;
- report accidental data sharing, account compromise or security concerns promptly;
- avoid posting internal church documents, discussions or decisions unless authorised.

Confidentiality is important, but it is not absolute. Information may need to be shared where there is a safeguarding concern, risk of harm, legal obligation, serious misconduct concern, pastoral necessity, governance responsibility or other proper reason.

St Peter's will also seek to identify and report fake, unauthorised or impersonating accounts, pages, groups or profiles which appear to represent St Peter's or which may mislead others, damage trust, create safeguarding concerns, or pose a risk to the church, its members, staff, volunteers or the public.

10. Moderation and unacceptable content

St Peter's may moderate, hide, remove or report online content on its official channels where it is inappropriate.

This may include content that is:

- abusive, bullying, harassing, threatening or discriminatory;
- sexually inappropriate, exploitative or unsafe;
- defamatory, malicious or knowingly misleading;
- a safeguarding risk;

- a breach of confidentiality or data protection;
- party-political campaigning on a church channel;
- spam, scam, impersonation or malicious software;
- contrary to St Peter's Christian ethos or policies.

Where serious or repeated concerns arise, St Peter's may restrict access to online channels, remove administrator rights, require inappropriate material to be removed, pause or end a volunteer role, take employment action, refer to safeguarding procedures, or seek diocesan, legal or police advice where appropriate.

Any request for passwords, devices, records or access to accounts must be handled lawfully, proportionately and with appropriate authority. St Peter's will not ask for access to personal accounts except where there is a proper legal, safeguarding, employment or governance basis and appropriate advice has been taken.

11. Conflicts of interest, payment and endorsement

Those covered by this policy should not use their connection with St Peter's to obtain personal benefit, payment, influence or endorsement through social media or online communication.

If someone is offered payment, sponsorship, benefits, gifts or hospitality in connection with online content relating to St Peter's, this may create a conflict of interest and should be declared in accordance with the Conflict of Interest Policy.

No one should imply that St Peter's endorses a product, service, organisation, campaign, political party or public statement unless this has been properly authorised.

12. Raising concerns

Concerns about social media or online communication should be raised promptly and appropriately.

Depending on the concern, the appropriate route may be:

- the person responsible for the account, group or ministry area;
- the Church Administrator;
- the Vicar;
- the churchwardens;
- the Parish Safeguarding Officer or Safeguarding Team;
- the Complaints Policy;
- the Whistleblowing Policy;
- the safeguarding procedure.

Safeguarding concerns must always be handled through safeguarding procedures.

Those who raise concerns in good faith should not be victimised or treated adversely for doing so. Equally, concerns should be raised truthfully, responsibly and without malice.

13. Related policies and documents

This policy should be read alongside, where applicable:

- Safeguarding Policy;
- Safer Recruitment arrangements;
- Code of Conduct;
- Welcome, Dignity and Fair Treatment Policy;
- Volunteer Policy;
- Staff Handbook and employment policies;
- Complaints Policy;
- Whistleblowing Policy;
- Conflict of Interest Policy;
- Data Protection Policy;
- Privacy Notice;
- Data Retention Policy;
- IT Security Policy;
- IT Acceptable Use Policy;
- Ministry Role Descriptions;
- relevant risk assessments and operational guidance.

14. Review

This policy will be reviewed by the PCC annually, or sooner if required by changes in law, Church of England guidance, diocesan guidance, safeguarding requirements, technology, parish practice or pastoral need.

The PCC is responsible for ensuring that this policy remains faithful to the doctrine and discipline of the Church of England, legally responsible, pastorally wise, practically useful, and consistent with St Peter's safeguarding, data protection and communications practice.

Short public-facing summary

Social Media Policy

St Peter's uses social media and online communication to share the gospel, welcome newcomers, encourage the church family and communicate well.

Those who use social media in connection with St Peter's should speak truthfully, kindly and wisely. They should protect confidentiality, respect safeguarding boundaries, use personal information carefully, and avoid anything that could harm others or damage trust in the church.

Official church accounts should be authorised, secure, appropriately monitored and used only for proper church purposes.

Adults acting on behalf of St Peter's must not use personal social media accounts to form private online relationships with children or young people connected with church activities. Online contact with children or young people must follow safeguarding procedures and be visible, accountable and properly authorised.

Church-related WhatsApp groups should have a clear purpose, appropriate administrators, and should normally be limited to those who currently need to be included for the purpose of the group.

Images, videos and livestreams must be used carefully, with appropriate consent, especially where children, young people or vulnerable adults are involved.

Safeguarding concerns must always be reported through St Peter's safeguarding procedures. They should not be handled merely as ordinary complaints, private disagreements or informal pastoral matters.