Darent Valley Community Church
Social Media and Online Safety Policy

Drafted: March 2024
Due for review: March 2025

Introduction
Digital technology is now a major part of daily life for most people and recent developments have enabled many new initiatives in the way churches use these technologies as part of their ministry. These create new and welcome opportunities to engage with people and to enhance communications, promoting greater inclusivity and cohesion within the church community. However, we recognise there are also risks associated with this. We should all pay attention to how we can safeguard each other, and especially children and adults at risk, to help ensure online safety.

This policy should be used alongside our *Safeguarding Policy* and our *Data Protection Policy*.

Aim and purpose of this policy
The aim of this policy is to promote healthy, safe and effective use of social media and digital technologies within the life and work of the church community and those that come into contact with us.

Who this policy applies to
• All those in positions of leadership and responsibility within the church
• Those involved in managing IT systems within the church
• All those engaged in any form of digital communication relating to church activities (both sending and receiving information).

Scope of the policy
The policy covers the following areas:

Understanding and recognising on-line abuse
IT systems and resources at DVCC
Electronic communications and use of social media.
Video conferencing.
Use of images and recorded video
Governance of the church website
Protocol for responding to online safety concerns
Resources for church workers using social media as part of their role

Definition of online abuse
All forms of abuse that may be facilitated through digital technology such as computers, tablets, mobile phones and any other internet-enabled devices.
Examples of online abuse include:

- bullying/cyberbullying
- sexting
- sexual abuse/exploitation
- emotional abuse
- financial exploitation
- scamming
- grooming
- harassment

It is possible that victims of online abuse may not always understand that they are being abused. However, the impact of such activities can be significant, particularly in the way it may create fear and isolation.

IT Systems and resources

This covers both the hardware and software used within the church, along with guidance about the use of particular apps, services or websites.
The church maintains a website (dvcc.online) which is hosted on the WordPress platform. Currently the church uses email and *WhatsApp* platforms. Some key personnel (staff and volunteers) have designated church email accounts.

At the point of the last review, the church possessed the following items of IT equipment which are located with church staff and volunteers to support their roles:

Device	Held by:	Purpose	Notes
Laptop 1	Pastor	Church related admin	
Laptop 2	Treasurer	Church Accounts/Songpro	
Laptop 3	Colin	The Space	
Laptop 4	Jason	Zoom/AV mixing	
Laptop 5	Steve	The Space	
Tablet 1	Jason	AV mixing	Damaged – not functional
Tablet 2	Colin	The Space	
Smart Phone 1	Pastor	Church related comms	

However, most of the church-related digital activity will be conducted via personally owned devices held by volunteers and the wider church community and its associates. We will maintain and use our IT resources to support good safeguarding practice.
This policy does not try to cover all aspects of IT use but highlights actions we will take to support safer practice. This will include:

- reviewing and updating the security of IT systems regularly (both church equipment and personal equipment used for church purposes)
- individual church members are asked to take measures to protect their personal IT equipment by installing anti-virus software and ensuring that these are updated regularly, thereby protecting the wider membership from computer viruses, malware, etc.
- risk assessing any emerging new technologies before they are used/endorsed within the church

• installing filtering software (to block inappropriate content) on devices owned and used by the church as appropriate
• reminding staff and volunteers of the need keep login and password details secure.
• passwords to church resources will be changed/updated whenever key personnel leave the organisation.
• password protecting spreadsheets containing personal data with access being restricted to those who's role it is to distribute communications from the church.

Individuals who use church-owned devices will be made aware of this policy and asked to comply with these guidelines for acceptable use. They will agree:

• not to search for and/or enter pornographic, violent, racist or hate-motivated websites
• not to retrieve, send, copy or display illegal or offensive material
• not to use obscene language
• not to violate copyright laws
• not to trespass in folders, work or files belonging to others
• not to harass, insult, bully or attack others
• not to damage devices, systems or networks
• not to use another user's unique password
• not to use computers for unapproved commercial purposes.

Electronic communications and use of social media (Good practice guidance for church-related digital communications)

The church aims to promote safe practice when using electronic communications and social media. This includes:

• using clear unambiguous language (avoiding 'text-speak') to reduce the risk of misinterpretation.
• avoiding communication after 10pm and before 8am
• keep 'data-heavy' communications to a minimum, especially where there is large group circulation (eg sending large numbers of pictures or large documents).
• obtaining parental/carer consent for social media contact with children under 16 years of age.
• using church accounts where possible instead of personal ones
• all social media interaction between workers (paid or voluntary) and children or adults at risk should be retained for reference if required, and should either:
    -specifically include another responsible adult (eg cc'd or added to a chat)
    -be subject to regular scrutiny by a responsible adult with oversite for the designated area of church activity.
• all participants must be above the minimum age limit for the social media platform being used (eg WhatsApp UK: aged 16+; Facebook UK and most other platforms: aged 13+)
• workers should ensure that their social media privacy settings prevent participants seeing personal information which is not linked to communication within the group.

• recipients of general circulation emails should be 'blind-copied' into the communication in order to protect their personal data.
• WhatsApp groups specifically set up for church purposes will be overseen by two 'administrators' who will modify settings and add/approve new members or delete those who wish to leave the group. The administrators will also be responsible for moderating content posted within the group. Content from invited individuals can largely be moderated via sensitive communication outside of the meeting/group. However, immediate action will be taken where *safeguarding/abuse/content that is not in keeping with the objectives of the charity as stated in its constitution* is identified by the moderator for the WhatsApp group:

Step 1 – ask the group member to remove/delete the offending message (can be done by the person holding finger on message and then selecting the 'delete' prompt.

Step 2 - an administrator of a group can delete other people's messages in the same way.

Step 3 – an administrator can remove someone from a group who repeatedly posts inappropriate content.

• All church workers (paid and voluntary) should be aware that statements and activities shared on personal social media may, by association, affect people's perception of the church. Church workers should ensure that content on their personal social media does not bring the church into disrepute, either through overt criticism of the church and it's leadership or by espousing views and behaviours that are markedly at odds with the beliefs and objectives of the church as stated in its constitution and policies.
• Key personnel (salaried and voluntary) should undertake an annual open source search (eg, via Google) for their name to check for identity theft, and seek to resolve any such on-line misuse.

Video conferencing/calls

We will create safe online spaces when using video conferencing or video calls. Currently the church uses the *Zoom* platform on which an account has been set up in the name of the pastor. The password for this account is held by those who are responsible for hosting church meetings. All meetings require the host to admit attendees from the virtual waiting room, thereby protecting bona-fide participants from malicious external interference.

One-to-one communication via video with a child or adult at risk is the equivalent of meeting that person in a room alone with no one around. Therefore, boundaries and safeguards should be in place, depending on the age or needs of the child or adult at risk.

For example:

• have an additional responsible adult physically in the room or included in the call with the child or adult at risk.
• ask a parent or carer to be present with the child or adult at risk
• keep a record of such meetings in which the following information is documented:

- date and time and length of the call,

- purpose and outcome of the call,
- specific disclosures or incidents which may pertain to safeguarding/on-line abuse.

Group video calls:

We will take appropriate measures to ensure the safety of participants in church related group activities conducted via video call or video conferencing. This will include:

- Communicating expectations for appropriate behaviour to participants
- When hosting group activities for young people:
  - there should be at least two adults on a call before a child (or adult at risk) joins.
  - organisational profiles and devices should be used wherever available rather than personal accounts
- Not recording group calls unless there is a compelling reason to do so.
- Appropriate safeguards will be applied when using recorded video:
  - anyone appearing in recorded video must provide appropriate consent
  - people will be informed if an event is being recorded and will be given an opportunity to move to a designated area where they will be out of camera shot.
- Church related video conferencing will use the Zoom platform.
  - A link to the event will be distributed to specific individuals for whom it is relevant and not placed on an open/publicly accessible platform (eg the church website or an open Facebook/Instagram/'X' [formerly Twitter] account).
  - Individuals will be admitted to the conference call by a responsible administrator.
  - The administrator will be able to mute or remove individuals from the call where this is deemed necessary *(eg. safeguarding/abuse/content that is not in keeping with the objectives of the charity as stated in its constitution)*
  - The administrator may terminate a video-conference if necessary (eg due to problematic behaviours within the call by multiple individuals).

Use of personal images

We will ensure the appropriate use of images taken during church activities. In relation to online use of images, this includes:

- ensuring appropriate consent is obtained before posting any images online
- ensuring that children or adults at risk cannot be individually identified by any personal details provided alongside the images
- discussion with parents and children about appropriate use of images eg where children may take pictures of each other during an activity.

Website

The church website provides an initial point of information for members of the public who are interested in churches in the Darent Valley and surrounding area. It provides

information about the nature of Darent Valley Community Church, its focus and leadership, as well as the activities it organises. Content uploaded to the church website is created and/or scrutinised and approved by the leadership team (eg. what's on, uploaded sermons, a photo gallery, and links to external material).
The church website includes a facility for comments and feedback by members of the public visiting the site. However, the WordPress platform on which the website is created, requires all such comments to be scrutinised and approved before being displayed publicly. The website administrator may seek support/advice from the church leadership team in reviewing/moderating public feedback to ensure that comments comply with this social media and online safety policy.

Responding to concerns
We will respond appropriately and sensitively to all online/social media safety concerns raised regarding church activities.

- In the event of concern that there may be an online safety incident of any kind, we will follow the process set out for responding to safeguarding concerns.
- If anyone is in immediate danger, this will be reported to the police or other statutory services straightaway.
- Serious incidents will also be reported to the Charity Commission.
- Other concerns will be reported to the Church Safeguarding Co-ordinator (CSC) who will determine what action is needed. If the CSC is unavailable, the matter will be reported to the Trustee responsible for Safeguarding.
- We will provide support to those affected, seeking advice from specialist services as required.
- An incident log of any digitally mediated concerns raised or identified will be maintained as part of the safeguarding policy. This log is reviewed as a standing item at Trustee meetings.

Resources
National Cyber Security Centre
Social Media: how to use it safely - NCSC.GOV.UK

Social Media and Children
How to deal with social media issues kids face online | Internet Matters

Government Guidance: Charities and Social Media
Charities and social media - GOV.UK (www.gov.uk)

Online Media – Literacy resources
Online media literacy resources - GOV.UK (www.gov.uk)

Key contacts
Church Safeguarding Co-ordinator
Sue Hart (Phone number: 07956590872; email address: DVCC.safeguarding@outlook.com)

Trustee responsible for Safeguarding

Steve Boddington (dvcc.eynsford@outlook.com)

Review
This policy will be reviewed annually and updated as required.

Date of most recent review:	25th March 2024
Date of next review:	March 2025
Signed and dated by:	Steve Boddington
(On behalf of the DVCC Trustees)	