Digital Safety Policy

ST JOHN'S CHURCH
LOVE • GROW • SERVE

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 technology as part of their ministry.

This opens up new and welcome opportunities to engage with people, but we recognise there are also risks associated with this. We should therefore all pay attention to how we can safeguard children and adults at risk to help ensure their online safety.

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

Aim and purpose of this policy:

The aim of this policy is to safeguard children and adults at risk when we are ministering on behalf of the church through the internet, social media, or mobile devices, and to provide guidance on our approach to online safety.

Who this policy applies to:

- All those in the church working with children and adults at risk
- Those involved in managing IT systems within the church
- All those engaged in any form of online ministry, including group activities.

All those working with children and/or adults at risk will be given – and asked to sign – copies of the relevant Codes of Conduct which include guidance about working safely online.

Scope of the policy:

The policy covers the following areas:

- IT systems and resources
- electronic communications and use of social media
- video conferencing
- livestreaming and use of recorded video
- appropriate use of images online
- responding to online safety concerns

Definition of online abuse:

Abuse that is facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices. It can happen anywhere that allows online digital communication.
Examples can include:

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

It is possible that victims may not always understand that they are being abused in this way.
The impact can be significant however, particularly in the way it may create fear and isolation.
We will maintain and use our IT resources to support good safeguarding practice. This covers both the hardware and software used within the church, along with decisions about the use of particular apps, services or websites. 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 our IT systems regularly
- risk assessing any emerging new technologies before they are used within the church
- installing filtering software on devices owned and used by the church as appropriate
- reminding staff and volunteers of the need keep login and password details secure

If the church runs activities (eg after-school club or a group helping adults get back into employment) where children or adults will be using church-owned devices, they will be made aware of what is acceptable usage and will agree not to:

- search for and/or enter pornographic, violent, racist or hate-motivated websites
- retrieve, send, copy or display illegal or offensive material
- use obscene language
- violate copyright laws
- trespass in folders, work or files belonging to others
- harass, insult, bully or attack others
- damage devices, systems or networks
- use another user's password
- use computers for unapproved commercial purposes.

We will promote safe use of electronic communications and social media:

This will include:

- using clear unambiguous language to reduce the risk of misinterpretation
- keeping copies of messages
- obtaining parental/carer consent for email or text contact with children
- avoiding communication outside of specific hours eg after 9pm
- using church accounts where possible instead of personal ones
- all social media interaction between workers (paid or voluntary) and children or adults at risk will be limited to church-administered groups
- all participants to be above the minimum age limit for the social media platform being used
- workers will take care with their social media privacy settings to prevent participants seeing personal information which is not linked to communication within the group

We will create safe online spaces when using video conferencing or video calls

One-to-one calls:

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. We will put appropriate boundaries and safeguards in place, depending on the age or needs of the child or adult at risk, for example:

- have an additional adult in the room with the caller
- ask a parent or carer to be present with the child or adult at risk

- keep a record of when meetings take place, length of meetings, frequency

Group video calls: We will take appropriate measure to ensure the safety of participants in our group activities via video call or video conferencing. This will include:

- Communicating expectations around appropriate behaviour to participants
- Ensuring there are at least two adults on a call before a child or adult at risk joins
- ensuring there are at least two adults on a call before a child or adult at risk joins
- using organisational profiles and devices wherever available rather than personal accounts
- not recording group calls unless there is a compelling reason to do so
- terminating a call if necessary (eg problematic behaviour by uninvited visitors)

We will apply appropriate safeguards when livestreaming or using recorded video.
This will include:

- ensuring anyone appearing in livestream or recorded video has given appropriate consent
- ensuring people know if an event is being recorded and giving them an opportunity to move to the designated area where they will be out of camera shot
- using group shots of the congregation and not singling out any individual

We will ensure appropriate use of images online:

We will follow our Safeguarding and GDPR guidance and 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

We will respond appropriately and sensitively to all online safety concerns:

In the event of concern that there may be an online safety incident of any kind, we will follow the Safeguarding Policy. If anyone is in immediate danger, this will be reported to the police or other statutory services straightaway. Other concerns will be reported to the Parish Safeguarding Officer (PSO), or their deputy, who will seek advice on what action is needed. We will provide support to those affected.

Key contacts:

Parish Safeguarding Coordinator: Nanette Wright
Data Protection Officer: William May

Review:

This policy will be reviewed annually, updated as required and adopted by the church meeting.
Date of most recent review: July 2025
Date of next review: July 2028