

Digital Safeguarding Toolkit for Churches

Protecting people digitally in church settings

SECTION 1

Introduction

What is digital safeguarding?

Digital safeguarding is the practice of protecting people from harm that can happen through online communication. For churches, that means thinking carefully about the messaging apps, social media accounts, video calls and group chats your community relies on to stay connected.

Churches are built on community, and digital tools have become a big part of how those communities stay connected. But they also introduce new risks that most churches haven't had to think about before: late-night messages that blur boundaries, private conversations with no oversight, personal phone numbers shared and sensitive discussions stored on platforms that were never designed with church life in mind.

Digital safeguarding is about making sure everyone in your church can participate safely.

Throughout this toolkit, we refer to your church's Designated Safeguarding Lead, or DSL. This is a named person in your church who is responsible for receiving and acting on safeguarding concerns. In the US, this role is more commonly called a Safeguarding Officer or Safe Environment Coordinator, but the responsibilities are the same. Not every church will have one, but section 7 covers the role in detail and explains why it matters. In the meantime, wherever we mention the DSL, think of it as whoever holds overall responsibility for the welfare of your congregation, whether that's your senior pastor, a board member, or another trusted leader.

Why it matters

Many churches already take physical safeguarding seriously, but a large number of those same churches have no framework at all for digital communication, even though a growing proportion of pastoral contact now happens online.

The reality is that most digital safeguarding failures don't come from bad intent. They happen because well-meaning people use familiar tools without stopping to think about the risks. This toolkit exists to close that gap.

Who this toolkit is for

This toolkit is for anyone involved in communicating within your congregation through digital channels including, but not limited to:



No prior safeguarding training is required. If you use - or plan to use - digital tools to communicate with the people in your church, this toolkit is for you.

This toolkit is intended as practical guidance to help churches think through digital safeguarding. It is not legal advice and should not be treated as a substitute for it. Safeguarding law and reporting requirements vary by country, region and denomination, so for advice specific to your church's situation, consult a qualified legal professional or your denominational safeguarding body.

SECTION 2

Understanding Digital Risk

Digital communication creates risks that can happen in churches every week, usually without anyone realizing.

*Scenario***Private messaging with no accountability.**

A youth leader starts texting a teenager from the youth group. The conversations are supportive at first but gradually become more personal and no one else can see these messages meaning there is no record, oversight or accountability.

*Scenario***Moving to personal platforms.**

A small group leader starts a group chat on a personal messaging platform (such as WhatsApp or GroupMe) to keep in touch with everyone. One of the members then sends them a private message through the same app. Just like that, the conversation has moved from a group setting into a one-to-one exchange with no audit trail and no boundary between the leader's personal life and their church role.

*Scenario***Late-night communication.**

A pastor receives a message at 11pm from someone in crisis and responds immediately from their personal phone, in bed. The conversation is well-intentioned but happens outside any professional framework so if a complaint arises, any record is limited to a private thread that may be deleted, inaccessible or lack context.

*Scenario***Emotional dependency.**

A volunteer builds a close pastoral relationship with a vulnerable adult through regular messaging, and over time the conversations become that person's primary emotional support. The volunteer is not trained to provide this level of care, so the relationship becomes unhealthy.

*Scenario***Data exposure.**

A church runs its volunteer group through a personal messaging platform, where every member can see each other's personal phone number. When someone leaves under difficult circumstances, they still have the personal contact details of all the volunteers on their device.

Why familiar tools create unfamiliar risks

The tools most churches default to for communication (iMessage, GroupMe, WhatsApp, Facebook Messenger, SMS, personal email) were all designed for personal use. None of them offer admin controls, audit logs, or any and no separation between personal and organizational communication.

This does not make them bad tools, but they are the wrong tools for communication where safeguarding matters.

SECTION 3

Code of Conduct for Digital Communication

These guidelines are for everyone who communicates digitally on behalf of your church, whether they're a paid staff member, a volunteer or someone in a leadership role.

✓ DO

✓ Use your church's chosen communication platform for all church-related messaging.

All church communication should happen on a purpose-built platform your church controls, with admin oversight and audit capability.

✓ Keep conversations visible.

Wherever possible, communicate in group settings rather than one-to-one. If a private conversation is necessary, make sure another leader is aware.

✓ Communicate during reasonable hours.

Unless there is a genuine emergency, keep messaging to normal waking hours. Acknowledge late-night messages briefly and follow up the next day.

✓ Maintain a clear boundary between personal and church communication.

Your church messages should not live alongside your family group chats and personal conversations.

✓ Be transparent about what you communicate and with whom.

If you would not be comfortable with your pastor, your safeguarding lead, or the recipient's parent reading the message, do not send it.

✓ Respond to pastoral needs within your training.

If someone shares something that's beyond what you're equipped to handle, connect them with your pastor, safeguarding lead or a trained professional.

✗ DON'T

✗ Message people under 18 or vulnerable adults privately using personal accounts or phone numbers.

All communication with minors and vulnerable adults should happen on a platform with organizational oversight, visible to at least one other adult leader.

✗ Move church conversations to personal platforms.

If someone tries to move a conversation to a personal messaging app or social media, bring it back to the platform your church has chosen.

✗ Share personal contact details through church communication channels.

Use the platform's built-in features. No one should need your personal number to participate in church life.

✗ Delete messages or conversations related to church communication.

If your platform provides an audit trail, do not bypass it. Records exist to protect everyone.

✗ Continue a conversation that makes you uncomfortable.

Let the person know you will follow up, and speak to your safeguarding lead.

✗ Assume that good intentions make risky behavior acceptable.

The majority of safeguarding concerns come from well-meaning actions, not malicious ones.

Why platform choice matters

Following these guidelines becomes much easier when your church uses a platform that was actually designed for organizational use. This should be a platform that focuses on:

Admin oversight

Not using or sharing personal information

Audit logs

Group-based communication

Clear data ownership

Jovo was built with exactly this in mind. It makes good safeguarding practice the default, rather than leaving it up to individual discipline.

The problem with personal messaging apps

Most churches communicate through whichever messaging tools people already have on their phones because they're free, they're familiar, and they're easy to set up. But none of them were designed for organizations that need oversight and accountability.

In a typical group chat on any of these platforms, members' personal phone numbers or contact details are visible to everyone in the group.

There is no admin dashboard, no audit trail accessible to the church, and messages live on personal devices outside any organizational data policy.

Jovo was designed to address these challenges. The app ensures:

- ✓ No personal phone numbers are required
- ✓ A centralized admin dashboard gives leadership clear visibility over groups
- ✓ Audit logs are available if a safeguarding concern ever needs to be reviewed
- ✓ When someone leaves, their access is removed cleanly

Choosing the right platform means making sure the tools you use support the care you already provide.

SECTION 4

Managing Online Spaces

**Messaging groups**

Every church messaging group should have a named moderator with admin-level access and a clear purpose. Make the purpose clear when the group is created and revisit it periodically.

**Social Media**

Church social media accounts should be managed by at least two people, and any direct messages received through those accounts should be treated as church communication rather than personal correspondence. Do not use church social media to communicate privately with individuals, especially young or vulnerable people.

This extends to personal social media accounts as well. Church leaders and those in positions of responsibility should never use personal social media accounts to initiate or maintain contact with young people, vulnerable adults, or members for church-related communication as this removes appropriate oversight and increases safeguarding risk.

**Livestream chat**

If your church livestreams services, assign a moderator to the chat. Livestream chats are public-facing and can attract inappropriate content from people outside your congregation, so active moderation is essential.

SECTION 5

Recognizing Concerns

Spotting safeguarding concerns online is harder than in person. You can't read body language through a screen, and you won't pick up on tone of voice in a text message.

Signs that something may be wrong

Secrecy.

A leader insists on using their personal phone to message someone rather than the church platform, or a young person mentions getting messages from a leader but asks you not to bring it up. Any time communication is being deliberately kept away from the people who should be able to see it, it's a cause for concern.

Escalation.

A conversation that starts out professional but gradually becomes more personal or emotional. Messages that get more frequent, start arriving late at night, or move from a group setting into a private channel.

Behavior changes.

A young person who becomes withdrawn after being in regular contact with a leader. Or someone who pulls away from church life altogether after a period of intense one-to-one interaction with a specific person.

Boundary violations.

A leader giving their personal number to a young person. A volunteer messaging people outside the church platform. A staff member having regular private conversations with a vulnerable person and no one else knowing about it.

Grooming patterns.

Grooming in digital spaces tends to follow a pattern: the person gradually isolates someone from group communication, builds emotional dependency through private messaging, slowly pushes past boundaries that would normally feel uncomfortable, and creates a sense of secrecy around the relationship.

Trust your instinct

If something feels off, don't dismiss it. You don't need to be sure that abuse is happening before you say something. Raising a concern isn't the same as making an accusation; it's a responsible step, and one that protects everyone involved.

SECTION 6

Responding to Concerns

If someone comes to you with a concern, or you notice something yourself that doesn't sit right, here's what to do.

If someone discloses a concern to you

- 1 **Stay calm.** This person is trusting you with something difficult, and how you respond in this moment matters.
- 2 **Listen.** Let them talk. Don't interrupt, and try not to ask leading questions or push for details. Your job right now is just to hear what they're telling you.
- 3 **Reassure them.** Let them know they've done the right thing by speaking up. Be honest that you won't be able to keep it to yourself, but explain that you'll only share it with the people who need to know so that everyone stays safe.
- 4 **Record what was said.** As soon as you can afterward, write down what they told you in their own words. Include the date, time and any relevant context. There's an incident report form in the Tools section that will help you capture everything in one place.
- 5 **Report it.** Pass it on to your church's Designated Safeguarding Lead (DSL) within 24 hours. If you believe a child is in immediate danger, contact the police first and then let your DSL know.
- 6 **Don't investigate.** This is important. Your role is to listen, record and report. Everything after that should be handled by people who are trained for it.

Emergency contacts

US: Call 911 if someone is in immediate danger. Childhelp National Child Abuse Hotline: 1-800-422-4453

UK: Call 999 if someone is in immediate danger. NSPCC Helpline: 0808 800 5000

Adults at risk: In the US, contact Adult Protective Services in your state.

In the UK, contact your local adult social care team.

What not to do

✗ Don't promise confidentiality.

It's natural to want to reassure someone, but you can't guarantee that a safeguarding concern will stay between the two of you. Make that clear from the start.

✗ Don't try to investigate it yourself.

It can be tempting, especially if you care about the people involved. But that is a job for trained professionals, and getting involved at this stage could actually make things harder for them.

✗ Don't confront the person the concern is about.

Even if you feel certain about what's going on, approaching them directly could put the vulnerable person at greater risk.

✗ Don't wait.

Report it within 24 hours. If someone is in immediate danger, act straight away.

SECTION 7

Roles and Responsibilities

Church leadership

Safeguarding is the responsibility of your senior pastor, board, elders or whoever forms the governing body of your church. That means making sure a policy is in place, a DSL has been appointed, the right communication platforms are being used, and that everyone on the team understands what’s expected of them.

Designated Safeguarding Lead (DSL)

Every church should have a named DSL. They’re the person who receives reports, works out what happens next, liaises with external authorities when needed, and keeps safeguarding records up to date. It’s important that your DSL has formal training and refreshes it regularly.

Staff and volunteers

If you communicate on behalf of your church in any digital setting, whether you’re paid or volunteering, you’re responsible for following the code of conduct in Section 3, knowing how to spot concerns (Section 5), and understanding what to do if something comes up (Section 6).

Platform administrators

Whoever administers your communication platform has a safeguarding role, whether they think of it that way or not. They control who has access, they can pull up communication records if a concern arises, and they’re responsible for removing people when they leave a role or the church.

SECTION 8

Quick Reference

“What do I do if...”

Use this table to find the right response quickly. In every case, your Safeguarding Officer or Designated Safeguarding Lead (DSL) is your first point of contact.

What’s happening?	What do I do?
Someone tells me about abuse or harm	Listen, record and report to your DSL within 24 hours. Do not investigate.
I see something concerning in a church chat	Screenshot it with date and time. Report to your DSL. Don’t confront anyone.
A young person messages me privately on my personal phone	Don’t continue there. Redirect to your church platform. Let your DSL know.
A leader asks me to keep our conversations secret from the church	This is a red flag. Report to your DSL immediately.
I’m not sure if what I’ve seen is serious enough to report	Report it anyway. It’s not your job to assess severity.
Someone is in immediate danger	Call 911 (US) or 999 (UK). Then inform DSL.

TOOLS AND TEMPLATES

Incident Report Form

When did the incident occur?

:

-

-

TIME

DATE

Your name:

Your role in the church:

Who is the concern about?

Role (if applicable):

Age (if known):

What happened?

Describe what you saw, heard or were told. Use their own words where possible.

Were there any witnesses?

☐ Yes

☐ No

If yes, please provide names and roles (if applicable).

Other than those involved and witnesses, is anyone else aware of the incident?

☐ Yes

☐ No

If yes, please provide names and roles (if applicable).

Has this incident been previously reported to the Designated Safeguarding Lead (DSL)?

☐ Yes

☐ No

If yes, please specify when this was reported.

Your signature

Date of Signature

-

-

Digital Safeguarding Checklist

- ☐ We have a designated safeguarding lead whose contact details are known to all staff and volunteers
- ☐ We have a written safeguarding policy that covers digital communication
- ☐ We use a communication platform with admin oversight and audit capability
- ☐ We do not allow one-to-one messaging between leaders and minors on personal platforms
- ☐ Personal phone numbers are not required or exposed through our church communication
- ☐ All messaging groups have a named moderator
- ☐ Access from communication channels is revoked when someone leaves a role or the church
- ☐ All staff and volunteers have read and agreed to our digital communication code of conduct
- ☐ We have an incident reporting process that everyone knows how to use
- ☐ Our safeguarding policy and toolkit are reviewed at least annually

Communication Boundary Checklist

A quick personal check-in for anyone in your church who communicates digitally on behalf of the church. Use it to reflect on your own habits and spot anything that might need to change.
Print a copy, work through the list honestly, and if you can't tick all of the boxes, have a conversation with your DSL about what to do next.

☐ All my church communication happens on our church’s official platform

☐ I do not message minors privately on personal apps

☐ I do not share my personal phone number through church channels

☐ My church messaging happens during reasonable hours

☐ I do not have private one-to-one conversations without another leader being aware

☐ I have not moved church conversations to personal platforms

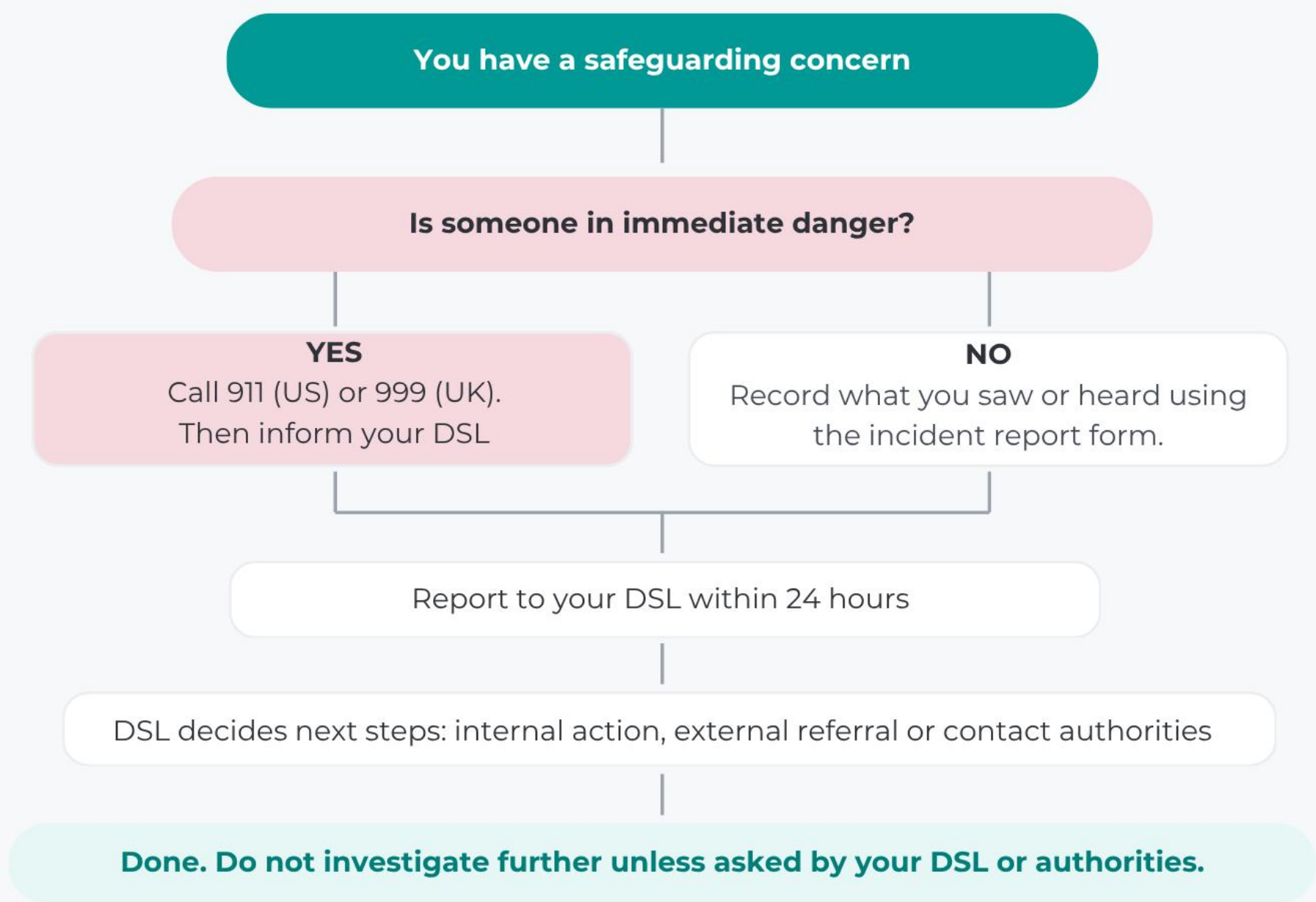
☐ I would be comfortable if my pastor or DSL read any church messages I have sent

☐ I know who my DSL is and how to contact them

If you can’t tick all of these, have a conversation with your DSL about what needs to change.

Reporting Flowchart

Use this flowchart when a safeguarding concern arises. Follow the path that matches your situation.



This toolkit is guidance only and is not a substitute for legal advice. Consult a qualified professional for advice specific to your church.



**Jovo is a secure team messaging app that centralizes
your communication and strengthens in-person connection.**

No personal phone numbers

Sign up with email only.

Centralized admin dashboard

Full visibility over groups.

Audit logs

Review communication if needed.

Group-based communication

No DMs by design.

GDPR compliant

Data hosted in London.

Church integrations

ChurchSuite, Planning Center.

Download free on iOS and Android

Available on the App Store and Google Play



GET IN ON
App Store



GET IN ON
Google Play

jovoapp.com