Technology Checklists for Churches and Conferences

Most churches run on a mix of staff, volunteers, and 'whoever knows the password.' That works—until it doesn't. When a pastor moves, a treasurer rotates, or a key volunteer steps away, it's easy to lose access to email, online giving, the website, shared files, or livestream tools.

This **two-part checklist** is meant to be practical. No technology jargon. Just a clear way to name what you have, keep access organized, and make transitions smoother—so ministry doesn't pause while you hunt for logins.

> *"A simple plan today can prevent a major disruption tomorrow."*

At a Glance

Part 1: Know What You Have	Part 2: Prepare for Transitions
• 1) Critical systems inventory • 2) Who has access (and why) • 3) Password & account plan • 4) Volunteer access guidelines • 5) Devices (church-owned & personal)	• 6) Files & records protection • 7) Website, domain & communications • 8) Giving & financial access review • 9) Offboarding (when someone leaves) • 10) Onboarding (when someone starts) • 11) Review schedule • 12) When to ask for help

Part 1: Know What You Have and Who Has Access

For pastors & ministry leaders: You don't have to be "techy" to do this. Think of it like stewardship—knowing what the church depends on and making sure it's not locked in one person's pocket.

For admins & tech volunteers: Use the checklists below as your baseline. Your goal is clarity: owners identified, access documented, and recovery options in place.

Checklist 1: Identify Your Critical Technology Systems

If the church would struggle to function without it, it belongs on the list.

☐ Ministry email accounts (staff, shared mailboxes, ministry aliases)

☐ Website, hosting, and domain name accounts

☐ Online giving platform(s) and donation processing access

☐ Financial software access points (as applicable)

☐ Social media accounts (Facebook, Instagram, YouTube, etc.)

☐ File storage (OneDrive, Google Drive, Dropbox, church server, etc.)

☐ Livestreaming, worship presentation, or media tools

☐ Wi-Fi, router, and network access information

☐ Church-owned devices (laptops, tablets, phones, cameras, etc.)

☐ Software subscriptions used by staff or volunteers

Checklist 2: Document Who Has Access

This is where most churches get stuck—because access is often informal. The fix is simple: **Please write it down.**

☐ Record who currently has access to each system

☐ Identify each person's role (pastor, treasurer, volunteer, communications lead, etc.)

☐ Note the level of access (owner, admin, editor, viewer, billing contact, recovery contact)

☐ Confirm access is tied to a ministry role—not just a person's preference

☐ Check whether former staff or volunteers still have access

☐ Assign someone to review and update access records

Optional table (print-friendly):

System	Who Has Access	Access Level	Ministry Role	Last Reviewed
Email				
Website / Domain				
Online Giving				
File Storage				
Social Media				
Wi-Fi / Network				
Livestream / Worship Tech				

Devices / Inventory				

Checklist 3: Create a Password & Account Management Plan

The goal isn't complexity—it's consistency. No critical account should depend on one person's memory.

☐ Decide where ministry passwords are stored (avoid texts, personal email, sticky notes, or unsecured spreadsheets)

☐ Use strong, unique passwords for each ministry account

☐ Enable multi-factor authentication (MFA) wherever available (call us for help if needed)

☐ Make sure recovery email addresses and phone numbers are current

☐ Avoid using personal email addresses as the primary owner of ministry accounts when possible

☐ Ensure more than one authorized leader can recover critical accounts

☐ Review passwords and recovery info during leadership transitions

Checklist 4: Volunteer Technology Guidelines

Volunteers are essential. Clear boundaries protect them and the church.

☐ Define which volunteer roles need technology access

☐ Give volunteers only the access they need to do their ministry work

☐ Avoid full administrator access unless truly necessary

☐ Create separate accounts for volunteers when possible instead of sharing one login

☐ Decide whether volunteers may use personal devices for ministry work

☐ Set expectations for storing, downloading, and sharing ministry files

☐ Clarify what to do if a volunteer receives suspicious emails, links, or messages

☐ Provide a simple handoff process when a volunteer rotates out of a role

Checklist 5: Manage Church-Owned and Personal Devices

A phone or laptop can carry more sensitive church information than a filing cabinet. Treat it that way.

☐ Keep a list of all church-owned devices

☐ Record who each device is assigned to

☐ Require passwords or passcodes on ministry devices

☐ Keep devices updated with current software and security patches

☐ Define whether personal devices may be used for ministry work

☐ Avoid storing sensitive information on unmanaged personal devices

☐ Remove church files and account access from devices when someone leaves a role

☐ Create a return process for church-owned devices

☐ Document who is responsible for checking devices after a transition

Part 1 quick win: Pick one system (email or online giving) and document owners + recovery contacts today. Small progress beats perfect plans.

Part 2: Prepare for Transitions and Keep Ministry Moving

For pastors & leaders: Transitions are normal. A simple offboarding/onboarding rhythm keeps ministry steady and reduces stress for everyone.

For admins & tech volunteers: Aim for repeatable steps: remove access, transfer ownership, verify recovery, and document what changed.

Checklist 6: Protect Files and Ministry Records

Make sure important documents live in ministry-owned spaces—not in someone's personal account.

☐ Identify where ministry files are stored

☐ Move important ministry documents out of personal accounts when possible

☐ Organize shared folders by ministry area or function

☐ Confirm that designated leaders can access critical files

☐ Review who can view, edit, or share files, give least privileges possible.

☐ Remove access immediately for former volunteers and staff

☐ Back up important files according to best practices

☐ Identify which records are sensitive and should have limited access

☐ Utilize Multi-factor Authentication, ask for help setting it up if necessary.

Checklist 7: Website, Domain, and Communications Access

Your website and social channels are often the first place people go for information. Don't let them hinge on one volunteer login.

☐ Identify who manages the website

☐ Identify who owns or manages the domain name

☐ Confirm domain renewal information is current

☐ Confirm billing information is connected to the ministry when possible

☐ Document who has access to website editing tools

☐ Document who has access to email marketing tools

☐ Document who has access to social media accounts

☐ Remove former staff and volunteers from communication platforms

☐ Confirm at least one current leader can post urgent updates

Checklist 8: Online Giving and Financial System Access

Handle these systems carefully and in coordination with finance leaders.

☐ Identify who has login access to online giving platforms

☐ Identify who has access to financial software

☐ Review whether former staff or volunteers still have access

☐ Confirm multi-factor authentication is enabled where available

☐ Limit access to those whose role requires it

☐ Document access changes when roles change

☐ Coordinate with finance leaders before changing access

☐ Review cybersecurity safeguards with the appropriate leaders

Checklist 9: Offboarding (When Someone Leaves a Role)

The key is speed and completeness—remove access, transfer ownership, and document what changed.

☐ Identify all systems the person had access to

☐ Remove or adjust access to email, files, website, social media, giving platforms, software, and devices

☐ Change shared passwords if shared access was used

☐ Recover church-owned devices and equipment

☐ Transfer ownership of important files or accounts

☐ Update recovery emails, phone numbers, and account administrators

☐ Confirm ministry communications will continue without interruption

☐ Document the date access was removed

Mini checklist (quick steps):

Transition Step	Completed?
Remove account access	☐
Recover devices	☐
Transfer files	☐
Update passwords if needed	☐
Check recovery settings	☐
Update the technology inventory	☐

Confirm who now owns the responsibility	☐

Checklist 10: Onboarding (When Someone Starts Serving)

Give access intentionally—not casually. It's easier to add access later than to undo the wrong access.

☐ Determine what systems the person needs access to

☐ Assign the **lowest access level needed** for the role

☐ Provide ministry-owned accounts where possible

☐ Explain password and security expectations

☐ Explain how files should be stored and shared

☐ Review expectations for personal device use

☐ Provide instructions for reporting suspicious messages or issues

☐ Record the date access was granted

☐ Set a date to review access if the role is temporary

Checklist 11: Schedule Regular Technology Reviews

Technology continuity works best as a rhythm, not a one-time project.

☐ Review technology access at least once per year

☐ Review access whenever key roles change (pastor, treasurer, communications lead, trustees, etc.)

☐ Review passwords and recovery settings regularly

☐ Review church-owned devices and inventory

☐ Review website, domain, and billing information

☐ Review social media administrators

☐ Review file storage permissions

☐ Confirm emergency contacts and recovery details are current

Suggested rhythm: Annually: full continuity review • Quarterly: quick check of critical systems • Immediately: after staff/volunteer transitions

Checklist 12: Know When to Ask for Help

If any of these are true, getting support is a wise next step—before a crisis forces the issue.

☐ No one knows who owns key accounts

☐ Former staff or volunteers still have access

☐ Passwords are shared informally

☐ Personal accounts are being used for ministry systems

☐ Backups or recovery information are unclear

☐ Leaders aren't sure whether systems are secure

Technology continuity is a form of faithful stewardship. When a church knows what systems it uses, who has access, and how transitions are handled, it protects people, information, and day-to-day ministry.

Keep this checklist somewhere easy to find, review it regularly, and update it whenever leadership changes. A little order now can save a lot of stress later.

> *"Faithful stewardship shows up in the small things—like keeping access clear and ministry moving."*