Archdiocese of Seattle

October 26, 2026

Network Equipment Inventory Advisory for Parishes and Schools

Oct 24, 2026 · @Kevin F. Benz

Purpose

Every parish and school in the Archdiocese of Seattle should build and maintain a written inventory of all equipment that connects to its network. This advisory explains what to list, what to record for each item, how to find every device, and which problems require immediate action.

Staff do not need IT training to complete this work. A parish office manager, school administrator or trusted volunteer can complete a first inventory in one to three days, depending on the size of the site.

Why the inventory matters

A site cannot protect, insure or replace equipment that it does not know it has.

- **Security.** Attackers commonly enter through devices that nobody updates or remembers: an old camera recorder, a forgotten web server, a copier with its factory password. On October 21, 2026, researchers disclosed the PHP2Shell flaws (CVE-2026-109618 and CVE-2026-109619) in web servers. A site with an accurate inventory can answer "Do we run anything affected?" in minutes. A site without one cannot answer at all.
- **Insurance.** Insurers and claims adjusters ask for make, model, serial number and purchase date after a theft, fire or flood. An inventory prepared in advance speeds the claim and supports the full replacement value.
- **Budgeting and replacement.** Purchase dates, warranty dates and end-of-support dates show which equipment the site must replace in the next one to three years. This allows the pastor, principal and finance council to plan costs instead of reacting to failures.
- **Incident response.** When a device misbehaves or a breach occurs, responders need to know what the device is, where it sits, who manages it and which vendor supports it. The inventory provides those answers immediately.

What to inventory

Include every device that plugs into the network or joins the Wi-Fi, whether the parish, the school, a vendor or a volunteer installed it. When in doubt, list it.

Category	Examples
Computers	Desktops, laptops, staff and lab machines
Servers and storage	File servers, web servers, NAS units, backup appliances
Network equipment	Firewalls, routers, internet modems, switches, wireless access points and controllers
Printers and copiers	Multifunction copiers, desktop printers, label printers
Phones	VoIP desk phones, phone system controllers, fax gateways
Cameras	IP cameras, NVR and DVR recorders
Physical security	Door access controllers, badge readers, alarm panels
Building systems	HVAC controllers, smart thermostats, bell and PA systems, lighting controls
Audio and video	Livestream encoders and cameras, sound boards, streaming PCs
Displays	Smart TVs, digital signage, projectors, classroom displays

Category	Examples
Student devices	Chromebooks, tablets, carts and their charging or management hubs
Vendor and cloud-managed devices	Anything a vendor installed or manages remotely, such as a copier lease, a security company recorder or a cloud-managed access point

Personal phones and guest devices do not need individual entries. Record instead that the site offers guest Wi-Fi and whether it is separate from the staff network.

What to record for each device

Record the following fields for every device. Leave a field blank rather than guess, and mark it for follow-up.

Field	What to enter	Where to find it
Device name	A short unique label, such as OFFICE-COPIER-1	Assign one; put the same label on the device
Type	The category from the list above	Visual inspection
Make and model	Manufacturer and model number	Label on the device or its settings screen
Serial number	The manufacturer serial number	Label on the back or underside
Location	Building and room	Walk-through
IP address and MAC address	The network address and hardware address	Router or firewall client list; device settings screen

Field	What to enter	Where to find it
Responsible person	The staff member who answers for this device	Pastor, principal or business manager decides
Vendor or support contact	Company, phone number, contract or account number	Invoices, service stickers, contracts
Firmware or OS version	The current software version	Device settings screen or vendor portal
Purchase date	Date bought or leased	Invoices, purchase records
Warranty end date	Date the warranty or lease ends	Invoice, vendor portal
End-of-support date	Date the manufacturer stops releasing updates	Manufacturer website or vendor
Internet-facing	Yes or No: can someone on the internet reach it directly?	Vendor, firewall settings, or ask the Archdiocese
Default password changed	Yes, No or Unknown	Vendor or whoever installed it
Notes	Anything unusual	Free text

Do not record passwords in the inventory. Store passwords in a password manager or another secure location that the Archdiocese approves.

How to find every device: step by step

Use several sources, because each one misses something. Compare the lists at the end and investigate any device that appears in one source but not the others.

1. **Assign an owner.** The pastor or principal names one person to lead the inventory and sets a completion date.
2. **Gather paperwork.** Collect invoices, purchase records, leases, service contracts and credit card statements from the last seven years. List every network-capable item they mention.
3. **Walk every room.** Visit each office, classroom, closet, sanctuary, hall, rectory and outbuilding. Look in ceilings, wiring closets, choir lofts and sound booths. Photograph each device label and record the device in the template.
4. **Read the router or firewall client list.** Sign in to the router or firewall (or ask the vendor who manages it) and export the DHCP client list. This list shows every device that received a network address, with its name, IP address and MAC address.
5. **Read the switch and wireless controller lists.** Managed switches and wireless controllers, including cloud-managed systems, list connected devices by port and access point. Export or photograph these lists.
6. **Check vendor portals.** Copier, phone, camera, door access and Chromebook management portals list the devices each vendor manages. Ask each vendor for a current device list if staff cannot sign in.
7. **Reconcile.** Match every address on the router list to a physical device. Treat any device that nobody can identify as a red flag and report it.
8. **Run a network scan only with approval.** A network scanning tool can find devices that the other steps miss. Do not run a scan without written approval from the pastor or principal and the Archdiocese IT contact, because scans can disrupt older equipment and may violate vendor contracts.
9. **Review and sign off.** The responsible person reviews the completed inventory with the pastor or principal and records the completion date.

Inventory template

Copy this table into a spreadsheet, or export this document to Word or PDF, and add one row per device. The first row shows a fictional example.



Technical Inventory Template.xlsx

Device name	Type	Make and model	Serial	Location	IP address	MAC address	Responsible person	Vendor or support contact	Firmware or OS version	Purchase date	Warranty end	End-of-support date	Internet-facing	Default password changed
SCHOOL-NVR-1	Camera recorder	Example Brand NVR-8000	SN123456	School, IT closet B2	192.168.1.50	00:11:22:33:44:55	Business manager	Example Security Co., contract 4471	4.2.1	2019-08-15	2022-08-15	2025-12-31	Yes	Unknown

The example device would trigger three red flags: it is past its end-of-support date, it is reachable from the internet, and nobody knows whether its default password has changed.

Keeping it current and storing it securely

An inventory is useful only while it is accurate. Treat it as a living record.

Keep it current

- Add a row the same day staff or a vendor installs a new device.

- Mark a row as retired, with the date and disposal method, when a device leaves service. Wipe or destroy storage before disposal.
- Repeat the router client list check (step 4) every quarter and investigate new, unknown devices.
- Complete a full walk-through and review every year, before the budget cycle begins.
- Update the firmware version field whenever staff or a vendor applies an update.

Store it securely

The inventory is sensitive. It shows an attacker exactly which devices exist, where they are and which ones are weak.

- Store it in an access-controlled location, such as the parish or school Microsoft 365 or Google Workspace account, shared only with named staff.
- Do not email it as an attachment, post it on a shared drive that volunteers can open, or store it on a personal device.
- Do not record passwords in the inventory.
- Keep one printed or offline copy in a locked location so that staff can use it during an outage or cyberattack.

Red flags to act on immediately

Do not wait for the inventory to be complete. Act on these findings as soon as staff discover them.

Red flag	Why it matters	Action
Default password not changed, or unknown	Manufacturers publish factory passwords online, and attackers try them first	Ask the vendor or installer to set a strong unique password this week
Device past its end-of-support date	The manufacturer no longer fixes security flaws	Disconnect it if possible, isolate it if not, and budget for replacement
Device reachable from the internet	Anyone can attempt to break in, at any hour	Contact the Archdiocese IT help contact before changing firewall settings

Red flag	Why it matters	Action
Web server or web-managed device on site	It may be affected by the October 2026 PHP2Shell flaws	Report it to the Archdiocese IT help contact and the vendor for patch confirmation
Unknown device on the network	It may be unauthorized or compromised	Do not unplug it yourself; report it with its IP and MAC address
No one responsible for a device	Nobody will patch or monitor it	Assign a responsible person