Printer security checklist

CHECKLIST

WHO CAN CHANGE THE PRINTER

- [ ] Change the default administrator password on every printer, and keep each one in the school's password manager.
- [ ] Turn off any guest or open access to the printer's settings page.
- [ ] Open the settings page over https where the printer offers it, not plain http.
- [ ] Write down who holds the administrator password, including the copier company's technician.

WHO CAN REACH IT ON THE NETWORK

- [ ] Put printers on their own VLAN or subnet, apart from student devices and guest wifi.
- [ ] Allow only the computers that send print jobs, and IT, to reach the printers across that boundary.
- [ ] Never forward a port from the internet to a printer.
- [ ] Give each printer a reserved or static address and record it in the printer inventory.

SERVICES TO TURN OFF

- [ ] List what each printer has switched on: IPP, IPPS, port 9100, LPR, FTP, Telnet, SNMP, WSD and any scan or email features.
- [ ] Turn off every service nothing in the school uses, one at a time, and print a test page after each.
- [ ] Where SNMP is still needed, use version 3 and turn off versions 1 and 2c.
- [ ] Prefer IPPS to plain IPP where the printer and the computers that print to it support it.

FIRMWARE

- [ ] Record each printer's firmware version from its configuration page.
- [ ] Each term, check the maker's website or the copier company for a newer version and for security notices on that model.
- [ ] Install firmware only from the maker or the copier company, never from a link in an email.

DOCUMENTS THE COPIER KEEPS

- [ ] Ask the copier company whether each machine stores jobs on an internal drive or memory.
- [ ] Turn on the drive's encryption or overwrite setting if the model has one.
- [ ] Before a copier leaves the building at the end of a lease or for disposal, have its drive wiped or removed, and get that in writing.
- [ ] Limit scan to email to addresses at the school's own domain, if the copier scans.

Free to copy, change and share.

PRINTER SECURITY LOG

Printer	Location	IP address	VLAN or subnet	Admin password changed	Services turned off	Firmware version	Firmware checked	Drive encrypted or wiped	Checked by