

CYBERSECURITY and DIGITAL INFORMATION POLICY

Saint Paul Area Synod

Adopted by Synod Council – March 12, 2026

Introduction

The Saint Paul Area Synod recognizes that significant information is entrusted to the staff of the synod. The Statement of Policy describes how the synod staff intends to maintain the secure storage of information in the digital age, recognizing that threats to an organization's integrity come in ever evolving ways. Central to this policy is a commitment to regular training in best practices and honest communication when breaches occur.

The Saint Paul Area Synod uses an off-site IT consultant to maintain its server and to oversee necessary firewalls and virus protection updates. Digital files are backed-up daily. Firewall parameters are set to allow website access to resources pertinent to the professional operation of the synod organization. The following types of sites are blocked: alcohol/tobacco, cult/occult, drugs/illegal drugs, gambling, illegal skills, intimate apparel, nudism, pornography, sex education, violence/hate/racism, and weapons.

Acceptable use of laptops, cell phones, and digital files

Use of synod-owned computers is limited to functions related to the work of the synod. It is the responsibility of each staff member to use synod resources and synod-owned technology in a manner consistent with the mission, ministry, and good stewardship of the church organization, as well as the security rules included in this policy or issued from time to time.

A laptop may be carried off-site during work-related travel or to one's home office with due diligence to protect the device from theft. Access to emails and files needs to be password protected. As much as possible, this will utilize a two-step verification process. Computer passwords will be updated every 90 days and will meet the criteria for strong passwords (combination of upper- and lowercase letters, numbers, symbols or special characters). Facial recognition software will not be installed.

Synod-owned cell phones are to be used for synod business only. Shared personal/business cell phones (with a portion reimbursed by the synod) are not to be used for purposes that would cause embarrassment to the synod or in any manner inconsistent with the synod's mission.

Personal information for fellow staff members, rostered ministers, or other leaders in the synod is not to be shared without explicit written permission from the bishop. The synod directory is password protected and accessible only to rostered ministers or congregational leaders by request. Sharing of any sensitive data must be done in a secure manner and consistent with this policy and security directives the synod may issue from time to time.

Login information is not to be automatically saved nor shared. The front office administrator will keep a copy of all logins and passwords in a locked file for use only in emergency situations.

Old computer equipment will be disposed of in a manner that protects against data loss or compromise (shredding, wiping devices, etc.).

Use of email system

Staff are to treat all email with suspicion, especially when a request claims to be urgent, involves money and/or contains links and file. If a staff member is unsure about the legitimacy of such an email, they should immediately discuss the matter with the bishop and/or other synod leadership. Staff should not under any circumstances reply to, or click a link, in a suspicious email. Requests for transfer of funds or other demanded action should not, under any circumstances, be acted upon without first validating the legitimacy of the request or demand.

Cyber attacks can also be initiated in the form of text messages or phone calls and these same rules apply to such circumstances.

Use of social media platforms

Access to social media for the synod is limited to the fewest number of staff and volunteers possible under the oversight of the director of communications. One back-up person shall have access as an administrator to cover social media postings in the absence of the director of communication.

Use of artificial intelligence

The synod recognizes the increased use of artificial intelligence (AI) in many forms of communication. While AI may provide benefits for the work and mission of the synod, AI also comes with risks. These include issues related to bias, privacy, data and other security and intellectual integrity and transparency. The synod is committed to ensuring that any use of AI is done in a responsible, human-centered, and ethical manner. At a

minimum, synod staff must disclose their use of AI, if used to summarize a meeting or to generate correspondence.

Banking and financial transactions

Access to on-line banking is limited to the synod's finance administrator, the bishop, and the synod's treasurer. All transactions require at least two persons in accord with the policies of the synod's banks and the ELCA's Mission Investment Fund. Passwords will be regularly updated, as requested by the financial institutions. Staff are prohibited from sharing their passwords with any other individual, whether on synod staff or a third party, except as described in this policy.

Reporting of data breaches

Any breach into the data-storage systems of the synod must be reported immediately to the bishop, the vice president of the synod, and the synod attorney. Law enforcement will be notified of such breaches involving personal or financial information. Such security breaches will be communicated directly to those whose information may have been compromised.

Training of staff

New staff hires will be trained in accord with this cybersecurity policy before gaining access to the data storage systems, email, and other digital resources of the synod. All staff will review the requirement of this policy at least once a year. Such training will include practice in spotting attempts at email hacking, phishing expeditions, and how to handle attachments from unknown sources.