

The policies outlined below pertain to the Southeastern Minnesota Synod, Office of the Bishop. The Office of the Bishop (referred to as "synod" in this document) is committed to providing an environment that encourages the use of computers and electronic communications as essential tools to support the mission and ministry of the Southeastern Minnesota Synod. In utilizing the synod's computers and electronic communications systems including, but not limited to, electronic mail and access to the Internet, it is important for all people using these systems to be aware of the policy regarding responsible use.

It is the responsibility of each synod employee (User) to ensure that this technology is used for proper business purposes and in a manner that (1) is responsible, professional, and legal; (2) does not compromise the confidentiality of proprietary or other sensitive information; (3) does not compromise the security of the synod's computer resources; and (4) is consistent with good stewardship and the mission and ministry of the Southeastern Minnesota Synod.

Acquisition and Use of Computer Resources.

- A. **Computer Resources.** The term computer resources includes, but is not limited to: all hardware (including personal computers, printers, scanners, servers, hand-held personal digital assistants, etc.), software, computer systems, data, information, electronic mail, instant messages, Internet services, and related systems.
- B. **Acquisition of Computer Resources.** All computer resources for the synod office shall be purchased by the Executive Assistant in consultation with the Communications Director and outside computer consultants used by the synod staff from time to time. Purchases will be within the budget for office equipment and will be researched to provide the best equipment at the best price. Any purchase in excess of \$250 will be capitalized in accordance with the capitalization policy.
- C. **Ownership of Computer Resources.** All computer resources provided to Users by or through the synod office are assets of and owned by the Southeastern Minnesota Synod. All User data, information, programs, electronic mail, graphic works, literary works, documentation, and other material created, received, sent or stored using synod computer resources, whether or not designated as private or confidential, are assets of and owned by the synod, not the individual User.
- D. **Systems Security.** It is the responsibility of every User to protect synod computer resources from unauthorized access, modification, destruction, or disclosure. Without limiting the foregoing, Users shall pay particular attention to the following:
 - 1. **Passwords.** Passwords are not required to use synod computers. There are some programs that require individual passwords to access the software. These passwords should be kept secure and given to other employees on a need to know basis. No User should attempt to obtain access to another User's documents or computer resources without prior authorization.

2. **Virus protection.** All files originating from sources outside the synod, including files obtained over the Internet, must be checked for possible computer viruses before being downloaded onto a synod computer. The virus-checking software on each synod computer will ordinarily perform this check automatically. If the virus checking software detects a virus, the User will receive a virus warning message. If this occurs, the User should request assistance from the Communications Director or the Executive Assistant in removing the infected files.
3. **Data Backup.** All Users should save important data and information to their designated location on the synod's network to assure it is protected, preserved, and recoverable in the event of a computer resource failure. The network is backed-up to assist in data recovery in the event of a computer resource failure.
4. **No Privacy.** Users do not have a personal privacy right in any matter created, received, sent, or stored on the synod's computer resources, whether or not the matter is designated as private or confidential. The synod reserves the right to monitor its computer resources and to read and copy all files or data contained on any computer resource including, but not limited to, e-mail messages and personal file directories, at any time and without prior notice. The synod reserves the right to access all computer resources for the purposes of supporting the mission and ministry of this synod.
5. **Software License Restrictions and Trademark and Copyright Laws.** Most proprietary software licenses have legal restrictions prohibiting unauthorized use and copying. Software may not be loaded, downloaded, or received on any synod computer including software available on the Internet, unless it is approved in advance by the Communications Director and the Executive Assistant. In addition, information posted, viewed, or downloaded from the Internet may be protected by copyright or piracy laws. Reproduction of protected information is permitted only if such reproduction is (1) permissible under applicable trademark, copyright and piracy laws, or (2) based on express permission given by the trademark or copyright owner. It is each User's responsibility to comply with applicable trademark, copyright, and piracy restrictions.
6. **Prohibited Uses.** It is the responsibility of each User to use synod computer resources in a manner consistent with the mission, ministry, and good stewardship of this synod. Without limiting the foregoing, Users shall not use synod computer resources in any way that:
 1. violates any law, statute, regulation or ordinance;
 2. violates any policy or procedure of the Southeastern Minnesota Synod;
 3. jeopardizes the security of any synod computer resource;
 4. jeopardized the tax exempt status of the ELCA, synod or congregation, or any affiliate listed under the ELCA Group Ruling for federal income tax exemption;
 5. violates the legal rights of any person or entity;
 6. creates unauthorized contractual liability for the synod;
 7. gives the impression a User is representing, giving opinions, making statements or commitments on behalf of the synod, unless authorized to do so by the Southeastern Minnesota Synod;

8. results in the transmission of obscene, pornographic, discriminatory, harassing, defamatory, or political or partisan campaign material;
9. interferes with the use of synod computer resources or the computer resources of another person or entity;
10. involves personal financial gain or gambling;
11. is inconsistent with norms of professional and business conduct;
12. reflects adversely on the Southeastern Minnesota Synod.

Responsible Use of the Internet

- A. **The Internet is for work-related purposes.** The synod's connection to the Internet is principally for work-related purposes through e-mail and access to the Worldwide Web. Unauthorized use of the Internet is prohibited. Unauthorized use includes, but is not limited to: (1) posting, viewing, downloading, or otherwise transmitting or receiving offensive, defamatory, pornographic, or sexually explicit material; (2) gambling; (3) engaging in computer "hacking" or other related activities; or (4) attempting to disable or compromise the security of information on any computer.
- B. **Participation in work-related Internet discussion groups is permitted with certain restrictions.** Users are responsible for ensuring that all information they share in work-related Internet discussion groups is accurate, and that any personal opinions they express are clearly identified as "personal" and not the opinion of the Southeastern Minnesota Synod. Such participation is allowed to the extent that it (1) does not reflect adversely on the synod and (2) is consistent with all the synod's standards and policies. Defamatory statements or written attacks are strictly prohibited.
- C. **Take precautions when providing information.** A User should never provide confidential, proprietary, or restricted information about the synod, its employees, congregations, members or rostered leaders without prior written consent.
- D. **Take precautions when obtaining information.** Information obtained from the Internet is not subject to quality controls and should be verified by an independent source before being relied upon.
- E. **The Synod may monitor Internet usage.** The synod reserves the right to monitor Internet usage at its discretion in the ordinary course of business.
- F. **Personal Internet usage.** Employees are not restricted from using the Internet for personal reasons. It is understood that personal use should not interfere with the official use of the Internet and may not be used for any activities prohibited by this policy. Employees should further understand that the bishop, executive assistant or the Executive Committee may monitor internet usage at any time, including personal use. Personal use is to be held to a minimum and, where possible, done on the employee's personal time.

Responsible use of e-mail.

- A. **E-mail defined.** For purposes of these policies, the term "e-mail" is any electronic message sent in any form from one computer to another including, but not limited to: (1) electronic mail; (2) electronic messages sent to chat rooms; (3) bulletin boards; (4) list servers; and (5) instant messaging.
- B. **E-mail is for business purposes.** The purpose of e-mail is to facilitate business communications among synod Users and to enable synod Users to carry out the duties of their positions. It is understood that personal use of e-mail should not interfere with the official use of e-mail and may not be used for any activities prohibited by this policy.
- C. **E-mail correspondence is the property of the Synod.** All e-mail correspondence is the property of the Southeastern Minnesota Synod, whether or not related to personal or confidential matters. The synod reserves the right to monitor its e-mail system, including a User's mailbox, at its discretion in the ordinary course of business. The existence of "passwords" and "message delete" functions do not restrict or eliminate the synod's ability or right to access electronic communications. In certain situations the Synod may be compelled to access and disclose messages sent over its e-mail system.
- D. **Offensive, demeaning, harassing, defamatory or disruptive e-mail is prohibited.** E-mail should conform to the same standards of propriety and respect as any other verbal or written business communication. Sending or forwarding offensive, demeaning, harassing, defamatory, or disruptive messages is prohibited. This includes, but is not limited to, messages that are inconsistent with the synod's policies as stated in the Personnel Policy Manual. Inappropriate use of e-mail may be grounds for discipline, up to and including termination of employment.
- E. **Users are responsible for eliminating inappropriate e-mail.** When receiving e-mail from outside sources, users have the responsibility of immediately deleting all e-mail that falls below the synod's standards as articulated above, including all pornographic, obscene, offensive, partisan political, and sexually explicit communications. Users also have the responsibility of ensuring that the prohibited e-mail is not seen by others. If the sender is a person known to the User, the User has responsibility of informing the senders of the e-mail that such communications are prohibited from synod premises and equipment and should not be sent in the future.
- F. **Creation and operation of list serves, bulletin boards and chat rooms.** A User may establish a list service, bulletin board, or chat room using the synod computer resources with permission of the Executive Assistant and/or the Executive Committee.

Web-Site Development, Content, and Security

The Communications Director of the Southeastern Minnesota Synod is responsible for development and maintenance of the synod's web-site. The synod's web-site is hosted by TDS Communications which also provides the synod's phone service. All web-site development must

conform to the specifications of TDS. Content is the sole responsibility of the Southeastern Minnesota Synod's Executive Committee and delegated to the Communications Director. Specific content is governed by the Publications Policy of the Southeastern Minnesota Synod.

All Users must comply with the Southeastern Minnesota Synod's Electronic Communications Policy. Violation of any of the terms of this policy may result in discipline, up to and including termination of employment.

*

* Congregations using this policy as a model will want to add a section covering computer use by congregation members.

Congregations are encouraged to install firewall, virus and spywear protection to computer systems. Data backup systems are also important for the safety of a congregation computer system.