St. Paul’s Evangelical Lutheran Church
Policy and Procedures

Usage of St. Paul’s Evangelical Lutheran Church Computers and Internet System

I. Policy

This policy is applicable to all members of the St. Paul’s Evangelical Lutheran Church community and staff.

This policy refers to all information resources, whether controlled or shared, stand alone, or networked. It applies to all computers and communication facilities owned, leased, operated, or contracted by St. Paul’s Evangelical Lutheran Church. This includes word processing equipment, personal computers, workstations, laptop computers, and associated peripherals and software, regardless of whether used for administration, research, teaching, or any other purpose.

Access to the information resource infrastructure within and beyond the St. Paul’s Evangelical Lutheran Church campus, sharing of information, and security of the intellectual products of the community all require that each and every user accept responsibility to protect the rights of the community. Access to the networks and to the information technology resources at St. Paul’s Evangelical Lutheran Church is a privilege and must be treated as such by all users of the system.

Anyone who accesses, uses, deletes, destroys, or alters any St. Paul’s Evangelical Lutheran Church information, resources, properties, or facilities without authorization, may be guilty of violating the privacy of others, of injuring or misappropriating the work produced and records maintained by others, and threatening the integrity of information kept within these systems. Purposely doing so is unethical and unacceptable.

II. Procedure

1. Staff are encouraged to use computers and the Internet to accomplish job responsibilities more effectively. Any use of St. Paul’s Evangelical Lutheran Church computers and Internet resources or systems, should reflect the sacred environment of our Christian community.

2. St. Paul’s Evangelical Lutheran Church reserves the right to screen computers to determine business appropriate usage at any time.

3. All assigned computers are to be pass coded. Each computer will be locked down at the close of business each day. The server system area will be secured when not in use.

4. All computers will have protective environment software installed. Attempting to override protective software is prohibited.

5. All users must conform to the legal restrictions, standards of conduct, and specific rules of etiquette when accessing the Internet.

Specific inappropriate conduct includes (but not limited to) the following:

- Use of the Internet for unlawful activities

- Use of the Internet for commercial activities not related to the organization

- Activities that interfere with the ability of others to make effective use of the network

- Violation of copyright, trademarks and licensing programs

- Intentionally accessing or downloading any text, picture (including video), graphic, or sound clip, or engage in any conference that includes material that is obscene, pornographic, libelous, indecent, vulgar, profane, lewd, or which advertises any product or service not permitted to minors by law

- Use of inappropriate language or language that is vulgar, profane, or lewd

- Sending of messages which include insulting or aggressive language, or expressions which are designed, intended, or likely to injure or harass others

- Sending of personal information about yourself or others

- Engaging in social "Chat Rooms"

4. Employee use of the Internet is a privilege, not a right, and may be revoked at any time for inappropriate conduct. Inappropriate or illegal use of the Internet may also result in disciplinary or legal action.

5. Vandalism will result in immediate cancellation of user privileges and will require restitution. Vandalism is defined as any deliberate attempt to harm or destroy data of another user, including (but not limited to) uploading or creation of a computer virus.

6. Violations may result in revocation of Internet privileges and any other applicable disciplinary action.

7. Staff must adhere to confidentiality and release of information policies when communicating on the Internet.

8. Staff must be aware that electronic mail is not private communication. Care must be taken to protect confidential information.

9. Staff are discouraged from downloading files from the Internet. Due to the fact that only a small quota is allocated to hold files, stored information should be kept to a minimum. Any files downloaded from the Internet must be scanned for viruses.

10. In the event that an inadvertent infraction occurs, the Senior Pastor is to be notified immediately.

I have read this policy and agree to follow these rules of conduct