St. Paul Lutheran Church
Student Acceptable Use Policy

1.0 Overview

St. Paul Lutheran Churchôs (hereinafter referred to as ñSt. Paulò) intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to St. Paulôs established culture of openness, trust and integrity. We are committed to protecting St. Paul's faculty members, students, the congregation and guests of the community from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet browsing, and FTP, are the property of St. Paul. These systems are to be used for educational purposes in serving the interests of the church and school, and of our students and congregation members in the course of normal operations.

Effective security is a team effort involving the participation and support of every St. Paul employee, member, and/or guest who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and/or information systems at St. Paul. These rules are in place to protect the students, parents/guardians, and St. Paul. Inappropriate use exposes St. Paul to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to students and parents/guardians of students at St. Paul. This policy applies to all hardware and software that is owned, leased, maintained, or operated by St. Paul.

3.1 Liability Disclaimer

Parents/guardians shall be liable, and hold St. Paul harmless, for userôs inappropriate use of electronic communication resources or violations of copyright restrictions or other laws, userôs mistakes or negligence, and financial obligations incurred by users. St. Paul shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.

4.0 Policy

4.1 General Use and Ownership

1. While St. Paul's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the information systems remains the property of St. Paul. Due to the need to protect St. Paul's network, administration cannot guarantee the confidentiality of information stored on any network device belonging to St. Paul.
2. Students are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, students should consult their instructor/teacher.
3. For security and network maintenance purposes, authorized individuals within St. Paul may monitor equipment, systems and network traffic at any time. Students

are prohibited from any type of monitoring of other students, equipment, staff, or other network traffic at all times.

4. St. Paul reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. Students should take all necessary steps to prevent unauthorized access to their personal information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Student level passwords should be changed whenever appropriate.
3. All Hosts should be logged off when unattended.
4. Any electronic communication by a student using a St. Paul Host is prohibited without expressed permission by the instructor/teacher.
5. All Hosts used by the students that are connected to the St. Paul Information System, whether owned by the student or St. Paul, shall be continually executing approved virus-scanning software with a current virus definitions unless overridden by St. Paul network or school administration. .

4.3. CIPA/NCIPA Compliant Notice

In accordance with requirements of the Childrenôs Internet Protection Act (CIPA) and the Neighborhood Childrenôs Internet Protection Act (NCIPA), all equipment connecting to the network from any connection located within St. Paulôs buildings will be blocked or filtered. St. Paul will make best efforts to prevent users from accessing or transmitting visual depictions of material deemed obscene, child pornography, and any material deemed harmful to minors as those terms are defined in CIPA. It will also make best efforts to prevent users from accessing or transmitting offensive, disruptive, or harmful data or any ñinappropriate matterò as that term is used in the NCIPA. This includes, but is not limited to, messages, files, or data that contain the following:

1. Pornographic or erotic images
2. Sexual implications
3. Racial slurs
4. Derogatory gender-specific comments
5. Information or instructions designed to cause harm to other person(s)/organization(s), comments that offensively address a personôs age, sexual orientation, beliefs, political beliefs, gender, religious beliefs, national origin or disability.
6. Any comment which in any way defames, slanders, or libels another person(s)
7. Any comment intended to frighten, intimidate, threaten, abuse, annoy or harass another person(s) or organization(s)

St. Paul acknowledges that no blocking or filtering mechanism is capable of stopping all inappropriate content all of the time. It is the responsibility of the staff to make best efforts to guide and to monitor students in the effective and appropriate use of St. Paulôs computer and information systems. This includes, but is not limited to:

1. Teaching students how to find educationally appropriate electronic materials.
2. Teaching students how to judge the educational suitability of electronic materials.
3. Teaching students information literacy skills, including understanding of safety, copyright, and data privacy.

4. Teaching students ethically, responsible, and appropriate behavior when accessing and communicating via the web.
5. Teaching students proper safety and security procedures when using email, online communities and collaborative workspaces, and other forms electronic communication.

4.4 Unacceptable Use

The following activities are, in general, prohibited. Students may never be exempted from these restrictions during the course of their enrollment.

Under no circumstances is a student authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing St. Paul-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by St. Paul.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which St. Paul or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate administration should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others.
6. Using a St. Paul computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction. This includes materials that are of a pornographic or sexual nature.
7. Making fraudulent offers of products, items, or services originating from any St. Paul account.
8. Effecting security breaches or disruptions of network services. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the student is not expressly authorized to access. For purposes of this section, "disruption" includes any use of network resources for malicious purposes.
9. Circumventing user authentication or security of any host, network or account.
10. Interfering with or denying service to any user other than the student's host (for example, denial of service attack).
11. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a userôs session, via any means, locally or remotely.
12. Providing information about, or lists of, St. Paul employees or students to parties outside St. Paul.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within St. Paul's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by St. Paul or connected via St. Paul's network.
7. Posting the same or similar related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.5. Blogging

1. Blogging by students, whether using St. Paulôs property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of St. Paulôs systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate St. Paulôs policy, is not detrimental to St. Paulôs best interests, and does not interfere with a studentôs normal curriculum. Blogging from St. Paulôs systems is also subject to monitoring.
2. St. Paulôs Confidential Information policy also applies to blogging.
3. Students shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of St. Paul and/or any of its students or employees. Students are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by St.Paulôs Non-Discrimination and Anti-Harassment policy.
4. Students may also not attribute personal statements, opinions or beliefs to St. Paul when engaged in blogging. If a student is expressing his or her beliefs and/or opinions in blogs, the student may not, expressly or implicitly, represent themselves as a representative of St. Paul. The student's guardian(s) assume any and all risk associated with student blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, St. Paulôs trademarks, logos and any other St. Paul intellectual property may also not be used in connection with any blogging activity.

4.6. Webpage Publishing

Students shall not publish any content publicly without expressed permission from their instructor/teacher to the Internet during school hours.

5.0 Enforcement

Any student found to have violated this policy may be subject to disciplinary action, up to and including expulsion.

5.1 Consequences of Inappropriate Use

The student and/or parent/guardian shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. Illegal use of the network, intentional deletion or damage to files or data belonging to others, vandalism to equipment or data, copyright violations or theft of services will be reported to the appropriate legal authorities for prosecution. General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use. Principals will administer penalties based on the severity and frequency of the offense.

6.0 Definitions

Term — Definition

Blogging — Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.

Spam — Unauthorized and/or unsolicited electronic mass mailings.

Host — Workstations, tablet PCs, smartphones, iPads/iPods, netbooks, notebooks, laptops

7.0 Revision History

Name	Purpose	Version
Brian Elmhorst/Teri Rae Suehs	Initial Policy	1.0

Student Acceptable Use Policy

St. Paul Lutheran Church

Use of computers and network at St. Paul Lutheran Church is a privilege that should be used to support learning appropriate for school. The smooth operation and maintenance of the computer system(s) relies on users adhering to established guidelines.

The student and his/her parent(s)/guardian(s) should be aware that St. Paul does not have control of the information on the Internet, but takes all measures possible to protect our children through internet filtering and education of ethical and appropriate use. Some sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate or potentially offensive to some people.

By signing this Student Acceptable Use Policy, students and parent(s)/guardian(s) agree to abide by the restriction outlined in this policy. The student and his/her parent(s)/guardian(s) of minors are responsible for setting and conveying the standards that their child should follow. Failure to return this agreement with signatures of both the user and parent/guardian will result in denial of access to the network.

I have read and understand the terms of St. Paul Lutheran Church Student Acceptable Use Policy and agree to those terms. I hereby give permission to issue an account for my child and certify that the information contained on this form is correct.

_________________________________ _______________
Student Name (please print) Grade

_________________________________ ________________
Student Signature Date

____
Parent/Guardian Name (please print)

________________________________ _______________ _________________
Parent/Guardian Signature Date Phone Number

*This agreement expires one year from date of parent/guardian signature above.