E-mail, and Internet Usage Policies for St. Philip Lutheran School 2017

The following represent policies currently in place on the use of Internet, and e-mail. Please refer to the Parent Handbook for policies related to personal electronic devices (e.g. cell phones, iPads, iPods etc…)

E-mail security policy

Purpose

This policy statement details the use and monitoring of electronic mail and mail systems.

Scope

The policies apply to St. Philip Staff and students, and cover e-mail located on St. Philip owned computers and servers. The policies apply to desktop and laptop personal computers as well as those attached to networks.

Specific policy

St. Philip property. As a productivity enhancement tool, St. Philip **encourages** the use of electronic communications (voice mail, e-mail, and fax). Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of St. Philip, and are not the property of users.

Authorized usage. St. Philip electronic communications systems generally must be used only for educational activities. Personal use is permissible so long as:

(a) It does not consume more than a trivial amount of resources.

(b) It does not interfere with Staff and students/student productivity.

(c) It does not preempt any educational activity.

Users are forbidden from using St. Philip electronic communications systems for private business activities, or amusement/entertainment purposes unless expressly approved by a member of the St. Philip staff. Staff and students are reminded that the use of these resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

Default privileges. All privileges on electronic communications systems will be assigned so that only those capabilities necessary to perform a task are granted. This approach is widely known as the concept of "need-to-know." For example, end users will not be able to reprogram electronic mail system software. With the exception of emergencies and regular system maintenance notices, broadcast facilities must be used only after the permission of a Staff member has been obtained.

User separation. These facilities will be implemented where electronic communications systems provide the ability to separate the activities of different users. For example, electronic mail systems will employ user IDs and associated passwords to isolate the communications of different users. But fax machines that do not have separate mailboxes for different recipients need not support such user separation. All St. Philip Staff will have unique usernames and passwords to access the e-mail system.

User accountability. Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions the other party takes with the password.

If users need to share computer resident data, they should utilize message-forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to electronic communications, it is recommended that users choose passwords that are difficult to guess (not a dictionary word, not a personal detail, and not a reflection of work activities).

No default protection. Staff and students are reminded that St. Philip electronic communications systems are not encrypted by default. If sensitive information must be sent by electronic communications systems, encryption or similar technologies to protect the data must be employed.

Respecting privacy rights. Except as otherwise specifically provided, Staff and students may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. St. Philip is committed to respecting the rights of its Staff and students, including their reasonable expectation of privacy.

However, St. Philip also is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

No guaranteed message privacy. St. Philip cannot guarantee that electronic communications will be private. Staff and students should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

Regular message monitoring. It is the policy of St. Philip NOT to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that ST. PHILIP will from time to time examine the content of electronic communications.

Statistical data. Consistent with generally accepted practices, St. Philip collects statistical data about electronic communications. As an example, call-detail-reporting information collected by telephone switching systems indicates the numbers dialed, the duration of calls, the time of day when calls are placed, etc. Using such information, Information Systems (IS) Staff monitors the use of electronic communications to ensure the ongoing availability and reliability of these systems.

Incidental disclosure. It may be necessary for a member of the Staff to review the content of an individual communication during the course of problem resolution. Staff may not review the content of an individual employee's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels.

Message forwarding. Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. St. Philips' sensitive information must not be forwarded to any party outside St. Philip without the prior approval of the Principal. Blanket forwarding of messages to parties outside St. Philip is prohibited unless the prior permission of the Principal has been obtained.

Purging electronic messages. Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. After a certain period—generally six months—electronic messages backed up to a separate data storage media (tape, disk, CD-ROM, etc.) will be automatically deleted by IS Staff.

Not only will this increase scarce storage space; it will also simplify record management and related activities. If St. Philip is involved in a litigation action, all electronic messages pertaining to that litigation will not be deleted until the St. Philip Principal or his/her designated representative has communicated that it is legal to do so.

Responsibilities

As defined below, the St. Philip Principal or his/her designated representative are solely responsible for electronic mail security have been so designated in order to establish a clear line of authority and responsibility.

1. Information Systems Personnel must establish e-mail security policies and standards and provide technical guidance on e-mail security to all St. Philip Staff and students.
2. Information Systems (IS) Personnel and students must monitor compliance with personal computer security requirements, including hardware, software, and data safeguards. Staff members must ensure that their students are in compliance with the personal computer security policy established in this document. IS Staff must also provide administrative support and technical guidance to management on matters related to e-mail security.
3. St. Philip Staff must ensure that:
    - Students under their supervision implement e-mail security measures as defined in this document.

Contact point

Questions about this policy may be directed to the St. Philip Principal or his/her designated representative.

Disciplinary process

Violation of these policies may subject Staff and students or contractors to disciplinary procedures up to and including termination.

Internet Security Policy

Purpose

The purpose of this policy is to establish direction, procedures, and requirements to ensure the appropriate protection of St. Philip information, content and equipment by Internet connections.

Scope

This policy applies to all Staff, students, contractors, consultants, temporaries, and other users at St. Philip Lutheran School, including those users affiliated with third parties who access St. Philip computer networks. Throughout this policy, the word "worker" will be used to collectively refer to all such individuals. The policy also applies to all computer and data communication systems owned by and/or administered by St. Philip.

Specific policy

All information traveling over St. Philip computer networks that has not been specifically identified as the property of other parties will be treated as though it is a St. Philip asset. It is the policy of St. Philip to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

In addition, it is the policy of St. Philip to protect information belonging to third parties that has been entrusted to St. Philip in confidence as well as in accordance with applicable contracts and industry standards.

Introduction

The new resources, new services, and interconnectivity available via the Internet all introduce new opportunities and new risks. In response to the risks, this policy describes St. Philip's official policy regarding Internet security. It applies to all users (Staff and students, contractors, temporaries, etc.) who use the Internet with St. Philip computing or networking resources, as well as those who represent themselves as being connected—in one way or another—with St. Philip.

All Internet users are expected to be familiar with and comply with these policies. Questions should be directed to the St. Philip Principal or his/her designated representative. Violations of these policies can lead to revocation of system privileges and/or disciplinary action, including termination.

Information movement

All software downloaded from non-St. Philip sources via the Internet must be screened with virus detection software prior to being opened or run. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone (not connected to the network) nonproduction machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

Unless tools like privacy enhanced mail (PEM) are used, it is also relatively easy to spoof another user on the Internet. Likewise, contacts made over the Internet should not be trusted with ST. PHILIP information unless a due diligence process has first been performed. This due diligence process applies to the release of any internal ST. PHILIP information (see the following section).

Users must not place St. Philip material (software, internal memos, etc.) on any publicly accessible Internet computer that supports anonymous file transfer protocol (FTP) or similar services, unless the St. Philip Principal or his/her designated representative has first approved the posting of these materials.

In more general terms, St. Philip internal information should not be placed in any location, on machines connected to ST. PHILIP internal networks, or on the Internet, unless the persons who have access to that location have a legitimate need-to-know.

All publicly writable (common/public) directories on St. Philip Internet-connected computers will be reviewed and cleared periodically. This process is necessary to prevent the anonymous exchange of information inconsistent with St. Philip ’s business.

Examples include pirated software, purloined passwords, stolen credit card numbers, and inappropriate written or graphic material (i.e., erotica). Users are prohibited from being involved in any way with the exchange of the material described in the last sentence.

Information protection

Wiretapping and message interception are straightforward and frequently encountered on the Internet. Accordingly, St. Philip secret, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods.

Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet.

Credit card numbers, telephone calling card numbers, log in passwords, and other parameters that can be used to gain access to goods or services must not be sent over the Internet in readable form. The PGP (pretty good privacy) encryption algorithm, or another algorithm approved by the St. Philip Principal or his/her designated representative must be used to protect these parameters as they traverse the Internet.

This policy does not apply when logging into the machine that provides Internet services. Currently ST. PHILIP does not use any type of encryption.

In keeping with the confidentiality agreements, St. Philip software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-St. Philip party for any purposes other than business purposes expressly authorized by management.

Exchanges of software and/or data between ST. PHILIP and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

Regular business practices, such as shipment of software in response to a customer purchase order, need not involve such a specific agreement since the terms are implied.

St. Philip strongly supports strict adherence to software vendors’ license agreements. When at work, or when computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.

Likewise, off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest, and are therefore prohibited. Similarly, reproduction of words posted or otherwise available over the Internet must be done only with the permission of the author/owner.

Expectation of privacy

Staff and students using St. Philip information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, Staff and students should not send information over the Internet if they consider it to be private.

At any time and without prior notice, St. Philip management reserves the right to examine e-mail, personal file directories, and other information stored on ST. PHILIP computers. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of ST. PHILIP information systems.

Resource usage

St. Philip management encourages Staff and students to explore the Internet, but if this exploration is for personal purposes, it should be done on personal time. Likewise, games, news groups, and other non-business activities must be performed on personal time.

Use of ST. PHILIP computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as no business activity is preempted by the personal use. Extended use of these resources requires prior written approval by the St. Philip Principal or his/her designated representative.

Public representations

Staff and students **may** indicate their affiliation with St. Philip in bulletin board discussions, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an e-mail address.

In either case, whenever Staff and students provide an affiliation, they must also clearly indicate that the opinions expressed are their own, and not necessarily those of St. Philip.

All external representations on behalf of the company must first be cleared with the St. Philip Principal or his/her designated representative. Additionally, to avoid libel problems, whenever any affiliation with St. Philip is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited.

Staff and students must not publicly disclose internal St. Philip information via the Internet that may adversely affect ST. PHILIP’s customer relations or public image unless the approval of the St. Philip Principal or his/her designated representative has first been obtained. Such information includes business prospects, unit costing, RFP information, and the like. Responses to specific customer e-mail messages are exempted from this policy.

Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, and related public postings on the Internet. If Staff and students aren't careful they may let the competition know that certain internal projects are underway. If a user is working on an unannounced product, a research and development project, or related confidential St. Philip matters, all related postings must be cleared with St. Philip Principal or his/her designated representative prior to being placed in a public spot on the Internet.

Access control

All users wishing to establish a connection with St. Philip computers via the Internet must authenticate themselves at a firewall before gaining access to ST. PHILIP’s internal network. This authentication process must be done via a dynamic password system approved by the St. Philip Principal or his/her designated representative.

Examples are handheld smart cards or user-transparent challenge/response. This will prevent intruders from guessing passwords or from replaying a password captured via a "sniffer attack" (wiretap). Designated "public" systems do not need these authentication processes because anonymous interactions are expected. Currently, ST. PHILIP does not use this system.

Unless the prior approval of the St. Philip Principal or his/her designated representative has been obtained, Staff and students may not establish Internet or other external network connections that could allow non-St. Philip users to gain access to ST. PHILIP systems and information. These connections include the establishment of multi-computer file systems (like Sun's NIS), Internet home pages, FTP servers, and the like.

Likewise, unless the St. Philip Principal or his/her designated representative, and legal counsel have all approved the practice in advance, users are prohibited from using new or existing Internet connections to establish new business channels. These channels include electronic data interchange (EDI) arrangements, electronic malls with online shopping, online database services, etc.

Reporting security problems

If sensitive St. Philip information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the St. Philip Principal or his/her designated representative must be notified immediately.

If any unauthorized use of ST. PHILIP's information systems has taken place, or is suspected of taking place, the St. Philip Principal or his/her designated representative must likewise be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the St. Philip Principal or his/her designated representative must be notified immediately.

Because it may indicate a computer virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like must also be immediately reported. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

Users must not "test the doors" (probe) security mechanisms at either St. Philip or other Internet sites unless they have first obtained permission from the St. Philip Principal or his/her designated representative. If users probe security mechanisms, alarms will be triggered and resources will needlessly be spent tracking the activity.

Responsibilities

As defined below, St. Philip groups and Staff and students members responsible for Internet security have been designated in order to establish a clear line of authority and responsibility.

a) Information Systems must establish Internet security policies and standards and provide technical guidance on PC security to all St. Philip Staff and students. The IS department must also organize a computer emergency response team (CERT) to respond to virus infestations, hacker intrusions, and similar events. The CERT Team is identified in ST. PHILIP's Personal Computer Security Policy.

b) Staff and students must monitor compliance with Internet security requirements, including hardware, software, and data safeguards. Program directors must ensure that their Staff and students are in compliance with the Internet security policy established in this document. IS Staff and students must also provide administrative support and technical guidance to management on matters related to Internet security.

c) Staff and students must periodically conduct a risk assessment of each production information system they are responsible for to determine both risks and vulnerabilities.

d) Staff and students must check that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.

e) Staff and students must check that user access controls are defined on these systems in a manner consistent with the need-to-know.

f) St. Philip information owners must see to it that the sensitivity of data is defined and designated on these systems in a manner consistent with in-house sensitivity classifications.

g) St. Philip Principal or his/her designated representative must ensure that:

1. Staff and students under their supervision implement security measures as defined in this document.
2. Staff and students under their supervision delete sensitive (confidential) data from their disk files when the data is no longer needed or useful.
3. Staff and students under their supervision who are authorized to use personal computers are aware of and comply with the policies and procedures outlined in all St. Philip documents that address information security.
4. Staff and students and contractor personnel under their supervision complete the pre-exit clearance process upon their official termination of employment or contractual agreement.

5. Staff and students and contractor personnel under their supervision make back-up copies of sensitive, critical, and valuable data files as often as is deemed reasonable.

h) Users of St. Philip Internet connections must:

1) Know and apply the appropriate St. Philip policies and practices pertaining to Internet security.
2) Not permit any unauthorized individual to obtain access to St. Philip Internet connections.
3) Not use or permit the use of any unauthorized device in connection with St. Philip personal computers.
4) Not use St. Philip Internet resources (software/hardware or data) for other than authorized company purposes.
5) Maintain exclusive control over and use of his/her/her password, and protect it from inadvertent disclosure to others.
6) Select a password that bears no obvious relation to the user, the user's organizational group, or the user's work project, and that is not easy to guess.
7) Ensure that data under his/her/her control and/or direction is properly safeguarded according to its level of sensitivity.
8) Report to the St. Philip Principal or his/her designated representative any incident that appears to compromise the security of St. Philip information resources. These include missing data, virus infestations, and unexplained transactions.
9) Access only the data and automated functions for which he/she is authorized in the course of normal business activity.
10) Obtain authorization for any uploading or downloading of information to or from St. Philip Principal or his/her designated representative.
11) Make backups of all sensitive, critical, and valuable data files as often as is deemed reasonable by their program director.

Contact point

Questions about this policy may be directed to the St. Philip Principal or his/her designated representative.

Disciplinary process

Violation of these policies may subject Staff and students or contractors to disciplinary procedures up to and including termination.

ST. PHILIP LUTHERAN SCHOOL COMPUTER CONSENT FORM

A SEPARATE FORM IS REQUIRED FOR EACH STUDENT!

Student Name____ Grade _________________

As the parent or legal guardian of the minor student(s) listed above, I grant permission for my son or daughter to use the classroom and lab computers on the campus of St. Philip Lutheran School.

I have read the above stated rules and accept responsibility for setting and conveying standards for my child to use the internet at St. Philip Lutheran School and in the home environment.

Parent Signature___________________________________ Date_____________________

Please Print

Parent Name____

E-Mail Address____

Please returned signed form to Mr. Oppermann no later than August 30, 2017

St. Philip Lutheran School Media Consent Form

A Separate Form Is Required For Each Student!

Student Name____ Grade __________________

As the parent or legal guardian of the minor student(s) listed above, I grant permission for my son or daughter to be photographed, videotaped, or appear in print or electronic media while attending The Lutheran School of St. Philip, 2500 W. Bryn Mawr Ave. Chicago, Illinois 60659. I hereby release, discharge and agree to save harmless The Lutheran School of St. Philip, its representatives, employees or any person or persons, corporation or corporations acting under its permission or authority, or any person or persons corporation or corporations, for whom it may be acting including any firm publishing and/or distributing the product, in whatever form, from and against any liability.

Parent Signature____________________________________ Date______________________

Please Print

Parent Name____

E-Mail Address____

Please returned signed form to Mr. Oppermann no later than August 30, 2017