Sacred Heart Information Technology Policies and Acceptable Use Policy

Overview

The Information Technologies Policies and Procedures is established to provide clear guidelines and expectations to staff and students at Sacred Heart School and Parish.

Sacred Heart is committed to protecting users from illegal or damaging actions by individuals, either knowingly or unknowingly. Network related systems, including but not limited to computer equipment, mulit-media equipment, phone systems, software, operating systems, storage media, mobile devices, network accounts providing electronic mail and or resources, WWW browsing, and FTP, are the property of Sacred Heart. These systems are to be used for educational and school business-related purposes with the intent of serving the interests of the students, teachers, and staff members of Sacred Heart and Parish.

Maintaining a network requires proper planning, organization, monitoring, and effective security. It is a team effort of all staff and students at Sacred Heart to meet and exceed the standards set forth by this policy along with State and Federal Law. It is the responsibility of every computer user to know these guidelines, and to govern themselves accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of the network-related systems within the Sacred Heart Campus. Inappropriate use, improper planning, and disregard of these procedures exposes Sacred Heart to risks including compromise of network systems and services, possible damage to the network, and legal issues.

Scope

This policy applies to all users of the Sacred Heart network. This policy further applies to all equipment that is owned or leased by Sacred Heart, including all future purchases.

Acceptable Use Policy

General Use and Ownership

Users should be aware that the data they create on the network remains the property of Sacred Heart. Users should have no expectations of expressed or implied privacy.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. In the absence of such policies, all questions will be directed to the Technology Director and or Director of Operations.

The use of the Sacred Heart network is a privilege. As with all privileges, it is the responsibility of the user to use this service appropriately and in compliance with all Sacred Heart polices to include state and federal regulations.

Sacred Heart assumes no responsibility for costs associated with loss or damage to devices not owned by Sacred Heart while on the network. The Technology Director must approve any non-Sacred Heart owned devices prior to connecting them to the network (LAN Connection). Users do not need permission to connect to the Guest Network.

For security and network maintenance purposes, the Technology Director may monitor equipment, systems, and network traffic at any time to help ensure the security and operation of the campus network.

Sacred Heart reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy in its effort to provide stable and functional network conductivity.

Security

Passwords, Accounts, and Antivirus

Users (Staff and Students) will be granted access to the network after they have signed the appropriate Network Usage Agreements forms and forwarded them to designated administrator (see Appendix A, Appendix B).

- Users must keep passwords secure and should not share their accounts. Authorized users are responsible for the security of their passwords and accounts.
- Users shall not leave computers unattended while logged on.
- Users will be required to change their passwords every 60 days.
- Passwords will follow guidelines to ensure a complexed password is utilized to provide the needed protection to school information.
- Users will not allow their username and password to be kept to automatically log into websites.
- Users must use extreme caution when opening e-mail attachments received from unknown senders, as they may contain viruses, e-mail bombs, Trojan horse code, ransomware, spam, or phishing messages with the intent to damage, hack or steal data from the Sacred Heart network.

- Users under no circumstances will create an account on a website for any school user under the age of 13 without signed consent from the parent or guardian prior to the account's creation.

Network Security and Administrator Rights

Administrative passwords for the network, servers, computers, wireless access points, and other electronic devices are to be kept strictly confidential. Distributing passwords of any kind is strictly forbidden.

Sensitive and Confidential Information

When handling sensitive and confidential information, precautions must be taken to prevent unauthorized access to the information. Staff members may not disclose sensitive information to persons not authorized to receive it. This includes non-public information such as Social Security Numbers, credit card numbers, bank account numbers, health information, or other confidential student and user data.

All users who have access to or may have access to Personal Identifiable Information shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Sacred Heart Policies, and all other applicable State and Federal laws and regulations, as they relate to the release of such information.

Protect printed sensitive data. Store sensitive data in locked desk, drawer or cabinet. Do not leave unattended sensitive data on desk, copier, FAX, or printer. Shred sensitive data that needs to be disposed.

Contact the school Principle or parish Director of Operations when questions arise regarding protected data.

Access and End User Support

Sensitive data access is restricted to only those personnel who need to perform their job duties. Access restrictions to such data are maintained by the IT Department in conjunction with the school Principle, parish Director of Operation, and Pastor of Sacred Heart.

Access to sensitive information is only granted with an accompanying and verifiable need. Reviews of accesses and privileges are conducted regularly and monitored to ensure compliance with all Sacred Heart Policies as well as State and Federal Laws and regulations.

Guest and Vendor Access

Guest and Vendor access can only be accessed through the wireless network and will remain separate from the main school network. Sacred Heart assumes no responsibility for costs associated with loss or damage to devices not owned by Sacred Heart while on the network. Sacred Heart is not responsible for any personal device's functionality.

Portable Device User Policy (Laptops\Tablets, etc.)

Users that are issued portable devices will be responsible for the security of the device while assigned to them whether on or off campus.

Users must understand that issued portable devices are property of Sacred Heart and must be returned in their original condition with all accessories upon request.

Users are financially responsible for damages and or loss due to negligence of portable equipment in their possession.

While portable devices are being used off campus, Sacred Heart has no control over the information accessed through the internet and cannot be held responsible for content viewed.

Revocation of privileges

Privilege and access to all Sacred Heart network devices, software, email, and information systems will be revised or revoked as necessary in the event of the following:

- Transfer of employee;
- Resignation of employee;
- Termination of employee;
- Suspension of employee;
- Or; when directed by Parish Pastor, Director of Operations, or Principle when revocation of privileges and access is deemed necessary.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host, if that host is disrupting production services).

Under no circumstances is an employee, student, or authorized guest of Sacred Heart authorized to engage in any activity that is illegal under local, state, federal or international law, while utilizing Sacred Heart-owned resources, to include the network, Internet and or computer platforms.

Users shall not access, download, store, send, or display text, images, movies, or sounds that contain pornography, obscenity, or language that offends or degrades others.

Attempts to circumvent or defeat mechanisms put in place by Sacred Heart to manage the network is strictly forbidden.

Users shall not attempt to download and/or install services, electronic file sharing mechanisms, games, software, tools, or any executable file including but not limited to the following file types: .exe, .bat, .cmd, .zip, .msi, and .rar.

***Note: The list below is not exhaustive, it does, however, provide a framework for activities which fall into the category of unacceptable use.**

Unacceptable Use: System and Network Activities

The following activities are strictly prohibited:

- 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 Sacred Heart;
- 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 Sacred Heart or the end user does not have an active license is strictly prohibited;
- The introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.);
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members;
- Using a Sacred Heart computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws;
- Utilizing Sacred Heart equipment and or networks for personal business use;
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to:
    - Accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;
    - Port scanning or security scanning unless prior notification and approval is received beforehand;

    - Executing any form of network monitoring, other than by IT personnel to manage network, maintain, and or troubleshoot;
    - Circumventing user authentication or security of any host, network or account;
- Providing information about, or lists of, Sacred Heart users to parties outside Sacred Heart without prior permission from the Director of Operations or Parish Pastor.
- Leaving computer logged in and unattended
- Leaving computer users account logged in overnight with webpages open. Best practice is that users will ensure to log out of their computers at the end of the day to ensure all internet connections are closed. (Note: Do not shut down computer overnight as updates are pushed to computer systems during off hours).
- Creating accounts for students on websites without requesting permission from school principal and having prior authorization from parent or legal guardian.

Unacceptable Use: Email and Communications Activities

- 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).
- Any form of harassment via email, telephone, text, SMS, or any social media outlets, whether through language, frequency, or size of messages.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Email

Staff and student emails are the property of Sacred Heart and are subject to review at any time as directed by the School Principle, the Director of Operations and or Parish Pastor.

Staff and student emails should not to be used for personal use and should always be considered official correspondence.

All employees of Sacred Heart will utilize their official email in correspondence with students and families. At no time will third parties or personal email or Websites, Facebook, Twitter, Snapchat, or similar communication programs be utilized without permission from the Schools Principal, Director of Operations, or Parish Pastor.

IT Technician Responsibilities

It is the responsibility of Sacred Heart Director of Technology to follow the guidelines and policies of the Sacred Heart School and Parish, and all State and Federal Laws to help provide a level of assurance to provide network protection. Sacred Heart IT makes a reasonable effort through use of teacher/staff overview, computer administration policies, Firewalls, Routers, and different web sense policies, programs, and equipment to ensure staff and students safety and security online, but will not be held accountable for any harm or damages that result from use of technology. The internet is an ever changing and growing flow of information and Every User must take responsibility for their use of technology and make every effort to avoid inappropriate types of content by following policies and acceptable use guidelines.

Security Incidents

Definition

A security incident is any violation of set Policies and Procedures that may or may not result in the following:

- Loss of information confidentiality (data theft);
- Compromise of information integrity (damage to data or unauthorized modification);
- Theft of physical IT assets including computers, storage devices, printers, etc.;
- Denial of service;
- Misuse of services, information, or assets;
- Infection of systems by unauthorized or hostile software;
- An attempt at unauthorized access;
- Unauthorized changes to organizational hardware, software, or configuration; and
- Reports of unusual system behavior, etc.

Response/Notification

- Staff and students who observe or experience a security threat in any form or believe data may have been compromised are to notify the Director of Technology immediately. If that person is not available the Director of Operations, School Principle, or Parish Pastor should be immediately notified.
- User should remove the affected device from the network.

Monitoring

Devices and Applications

In an effort to maintain network security, integrity, and to reduce the risk of Security Incidents the IT Department, at the discretion of the Director of Technical Support Services, can and will monitor network activity. These monitoring devices/applications include but are not limited to:

- Firewall logs;

- Web Filtering logs;
- Network Traffic Monitoring;
- Active Directory Monitoring;
- Mail Scanner logs;
- Database, backup, and usage logs on servers; and
- Event logs and histories created in individual machines.

Files and Correspondence

- In the course of their duties, it may be necessary for the Director of Technology to view files, data or communications that have been stored by users on devices or network file servers. The viewing of such material is permitted only when it is necessary to troubleshoot problems at the request of the user, protect the security and integrity of the Sacred Heart network, protect the rights or property of Sacred Heart, or to ensure compliance with Sacred Heart policy or applicable laws.
  - Examples include:
    - The identification/restoration of lost, damaged or deleted files;
    - The identification of a process that is interfering with normal network functions; or
    - In more serious circumstances, an investigation of a Security Incident.
    - In all such cases, consideration of the confidential nature of files and/or communications that may potentially be reviewed and shall implement the appropriate safeguards to ensure that all local, state and federal privacy laws are complied with.

Disposal of Technology Equipment

- All technology equipment must be disposed of in a manner that adheres to Sacred Heart Policy to ensure the protection/destruction of any data on the Harddrive's and RAM.

Enforcement

Failure to adhere to these policies and guidelines by Sacred Heart employees can result in suspension up to and including termination, revocation of the offender's privilege and access to the network and/or other disciplinary or legal action determined by parish management.

Revisions

Sacred Heart School/Parish reserves the right to revise these policies and procedures at any time to ensure the operability and safety of the network and its users.

Appendix B

Student Network/Internet Acceptable Use Policy

Parent or Guardian Network/Internet Acceptable Use Policy

As the parent or guardian of ____, I have read the Terms and Conditions of Sacred Heart's Information Technology Policy (located at www.shsreedsburg.org\resources). The Internet is an information highway connecting thousands of computers all over the world. I understand that my child will have access to the Internet and with this access comes the availability of some material that may not be considered to be of educational value within the context of the school setting. I understand that internet access throughout the school is designed for educational purposes and that some materials on telecommunication networks may be objectionable.

Efforts will be made to direct students to educationally related material. However, on a telecommunications network(s) it is impossible to control all materials and sites. I believe that the valuable information and interaction available on the network(s)/Internet services far outweigh the possibility of users gaining access to sites that are not acceptable.

I understand that violation of the guidelines established by Sacred Hearts Information Technology Policy will result in the students access to the network being suspended and parent/guardian being notified.

Sacred Heart School utilizes Go Guardian as an additional administrative resource in the classroom in an effort to keep network access monitored and managed for our students. Go Guardian monitors internet activity and computer usage of all Chromebooks and students school account when logged in. Note, if a student is logged into their school google account from a personal computer, URL access may be tracked and recorded by our Go Guardian account. No private information is being collected, only the access to URL, date/time.

Student Name Printed: ____________________________________

Grade: ______________ School Year: __________________

Parent/Guardian Name (Please print): ____

Parent/Guardian Signature: ____

Date: _____________