SUMMIT CHRISTIAN ACADEMY

INFORMATION SECURITY POLICY

INTRODUCTION

The Summit Christian Academy (SCA) Information Security Policy defines the fundamental principles for the protection of the school's information resources, the proper controls needed to ensure compliance with internal and external regulations, and to uphold the school's reputation with its school families and the community. All board members, administration, faculty, staff, external vendors, volunteers, and students are responsible for ensuring compliance with the SCA Information Security Policy.

MISSION STATEMENT

The mission of Information Security is to protect the confidentiality, integrity, and availability of the school's information infrastructure and resources through the establishment, implementation, and management of the Information Security Program. This involves creating, administering, and overseeing policies to ensure the prevention, detection, containment, and correction of security breaches.

PURPOSE

The purpose of the Information Security Program is to ensure that school Administration, Accreditations Teams, and any regulators are satisfied with the security controls that the school has implemented, and that students, parents and business partners are confident their information is adequately protected.

RESPONSIBLE PARTY

The SCA Board of Education has designated Dan Cockrell, Technology Director, to implement, supervise, and maintain the WISP. This employee, (hereafter referred to as the "Technology Director") will be responsible for the following:

A. Implementation of WISP
B. Training of all new employees or his designee
C. Annual testing of the WISP safeguards
d. Evaluating any external vendor's ability to adhere to this policy
E. Reviewing the scope of security measures annually at minimum, but also when a change in the operations of the business deems it necessary
f. Annual Refresher Training of WISP will all faculty, staff, vendors, volunteers, and

administration

EXCEPTIONS

Unless noted specifically in the WISP, any exceptions to this policy must be granted in writing. This written approval be from the Technology Director AND at least one other member of Administration (Elementary or Secondary Principal Director of Operations, or School Administrator, or Academic Dean)

POLICY DETAILS

CLASSIFICATION OF DATA

Level of sensitivity	**Type of data**	**Level of protection**
Level 1 Highly sensitive and mission critical information for limited consumption.	Child protection/legal matters Behavior logs and discipline records Student personal information Staff personal information Family Financial Information	Not available beyond School buildings. Electronically encrypted with limited access to need to know parties only
Level 2 Essential to the successful running of the school, much of which can be accessed via the private side of the schools own learning platform (Facts SIS)	Student Attendance information Staff Performance Management information Staff profiles and performance reviews	Teacher access Login password Limited to own classes/students Password on specific teacher, department or class files / folders Student access Login only to their own progress records Parent/Guardian access

	Student Individual Education Plans, School Financial information	Login to own child(ren) records only
<u>Level 3</u> Much is in the public domain and accessed via the public facing website (sca-kc.org) or learning platform (Facts SIS).	Lesson plans Teaching notes School calendar, staff bulletins School policies and procedures Student work Student learning logs General school / class letters Student photographs (parental consent)	Student or Parent login Password on student specific files / folders

Data has been assigned three possible Levels, Level 1 being the most sensitive, and Level 3 being the least sensitive. If not specified in this policy, sensitive data is defined and either Level 1 or 2, and non-sensitive data as Level 3. Any data not specified should be treated as sensitive Level 2 until classification of such data can be determined.
Sensitive Information is information about a person or an entity that, if disclosed, could place either the person or the entity at risk of criminal or civil liability, or be damaging to financial standing, employability, or reputation. SCA is bound by law or by contract to protect some types of sensitive information. Additionally, SCA requires protection of some other kinds of information beyond legal or contractual requirements as an additional safeguard.

Access Control

SCA Domain access shall be granted to all faculty, staff, and students. The level of access should be granted to users based on business and/or academic need. Access permissions

should not exceed the requirements for a user's job or educational function. Final determination of access controls are determined by Technology Director.
Each user is given a unique set of credentials in order to access protected systems. Users should never under any circumstances ever share their username or password information with anyone. Users will be held responsible for actions performed under their user ID. Shared user accounts, such as "Guest" are not allowed.
User accounts are to be terminated/deactivated when a user is longer a student or staff member of SCA. This should occur immediately upon termination of employment/relationship with SCA.

Confidentiality of Information Security Framework

SCA Information Technology does not disseminate any information pertaining to the architecture and/or security of the network to any parties either by verbal, written, or electronic means. In certain cases, consultants, vendors and others may have access to this information. No SCA staff shall divulge any aspect of the IT Infrastructure without the express consent of a member of the Technology Director.

Fixed Password Management

All fixed passwords must be at least eight characters, and where systems support it, this minimum length must be enforced automatically. Users must also choose fixed passwords that include any two of the following

- alphabetic characters
- numeric characters
- symbol characters

User-assigned fixed passwords should not be reused or recycled. Where systems support it, fixed passwords must be forced to change every ninety (90) days. Likewise, where systems support it, expired passwords must be maintained and not allowed to be reused. If any user suspects that somebody else may know their password, the passwords must be changed immediately. Faculty and Staff users forgetting their passwords must contact a systems administrator or technology directory for password resets.
Exceptions to Password Policy:
a. Due to the vast number of students forgetting passwords and the high volume of reset requests in the past, all student passwords are to be set by the administration at the beginning of the school year. Password lists are provided to technology staff, and appropriate faculty members to assist students with login as needed. All faculty and staff must treat this password list as confidential and is not to be shared with a volunteer, substitute teachers, or other staff members. All students' passwords will be reset at the beginning of each semester.

b. Facts SIS: Facts SIS is a system used by SCA to allow parents to view student grades and keep track of student financials (Lunch and Tuition balances). Parent accounts are deactivated each summer, approximately two weeks after the conclusion of the school year. All parent passwords are to be reset annually and require parent accounts to change their passwords immediately upon login at the beginning of each school year. Maintenance and backups of

Facts SIS are the responsibility of Joe Hesman, Kreg Welch and Joe Sanders. It is the responsibility of the Technology Director to receive confirmation that such backs ups are occurring regularly.

Conduct/Behavior

Frivolous, disruptive, or inconsiderate conduct in the computer labs or at any SCA computer areas is not permitted. Students may not use the computer in the computer lab or library without faculty supervision. No SCA IT system may be used for playing computer games unless approved by supervising teacher as having educational value.
All users are required to lock their computer before stepping away from the terminal. This prevents unauthorized access by other users.
All computers should be left powered on at the end of the day to ensure that updates can be automatically installed overnight.

Personal Drives

All Faculty, Staff, and Students will have a personal drive that can be accessed from any computer on the SCA domain. Personal drives should not contain any sensitive (Level 1 or 2) data regarding student personal contact information, student grades, or future or past exams. Faculty should store sensitive data on network drives to ensure proper protection and backup of data.
SCA IT does not allow storage of non-work or non-class-related personal data such as audio files, audiobooks, movie or video files, or image files on the SCA servers. SCA IT periodically conducts audits of disk space usage. If SCA IT notices that a user has excessive storage of non-work or non-class-related audio, image, or movie files stored in their personal drive, they will be asked to remove this data, or in some extreme cases, the data may be removed without notification of the user. All student personal drives will be erased at the end of each school year.

Network Drives

Network Drives will be used for sensitive (Level 1 or 2) information and storing files related to a specific class or group. Files saved in a network drive are the property of Summit Christian Academy. For non-sensitive (Level 3) information, SCA IT recommends sharing files with Google Apps for Education or Facts SIS. All students have a Gmail based student email account. All parents/guardians have access to Facts SIS.

Email

Faculty and Staff member will be issued a sca-kc.org email address, which can be managed through either Facts SIS or Gmail. SCA IT recommends that faculty use Gmail to take full advantage of the Google Apps for Education functionality which will enable easy file sharing with students.
All students will be issued a realschoolspirit.org email address, which is managed through Gmail.

Users are to take precautions to prevent the unauthorized use of e-mail account passwords. Passwords are not to be shared with others and their confidentiality is to be strictly maintained. Users will be held accountable for all actions performed with their passwords, including those performed by other individuals as a result of user negligence in protecting passwords. SCA IT and support staff will not ask you for your password. No one is to use another individual's account, with or without permission.
All mail messages originating from sca-kc.org and realschoolspirit.org email addresses are the property of Summit Christian Academy. SCA cannot guarantee the security, privacy, and confidentiality of email. Users should not assume confidentiality of their email. Users are advised not to send Level 1 or 2 category data in email communications.

Personal Devices and Wireless Access

No personal devices, including smart phones, tablets, laptops, and desktop systems may access the SCA domain.
A guest Wifi is available for visitors and guest of Summit Christian Academy. Access to the Wifi is determined by the Administrative Staff and the Technology Director. The SCA Wifi network utilizes an encrypted authentication process (WEP) in order to get access. Once authenticated, traffic is not encrypted. The SCA Wireless network is to be used for non-sensitive (Level 3) data only. Users of the SCA Wireless network are strongly discouraged from using it for any credit card or financial transactions. Wifi does not have access to any SCA network resources. The Wifi password is to be changed every thirty (30) days.

Portable Devices Owned by SCA

Under no circumstances should any portable device contain Level 1 data. All portable devices must have encrypted hard drives. Since at this time only administrative staff is using iPads and laptops, Level 2 data is allowed on portable devices. All school iPads must have remote wipe capabilities (Find my iPad) activated.

Personal Use of SCA Information Systems

All User activity is subject to logging and subsequent analysis. Users must not perform any activity on SCA information systems that could damage SCA hardware, software, or network infrastructure. Unbecoming conduct could lead to disciplinary action including revocation of access control privileges. Incidental personal use of SCA information systems is permissible so long as the usage does not interfere with job performance, does not deny other users access to the system resources, and does not incur significant costs. Personal use of SCA information, such as a mailing list, is prohibited.
Users must not test, or attempt to compromise any information security mechanism unless specifically authorized to do so by the Information Technology Department. Users are prohibited from possessing software or other tools that are designed to compromise information security on school property. (For example, password cracking software).

Viruses and Malicious Software

All hardware connected to the SCA domain must have virus protection installed and up to date. All security patches for software and operating systems must be installed regularly. Spyware scanning software should also be installed and up to date.
SCA IT discourages transferring and using CDs, USB Drives, DVDs from home to school or from school to home. This practice will assist in the elimination of potential virus outbreaks. SCA IT realizes that sometimes exceptions will occur. The approval of using an external CD/USB/DVD is required. Supervising teachers can grant an exception to this rule with a verbal acknowledgement. All CD/USB/DVD must be scanned by virus software prior to use.
SCA IT will perform monthly audits of random systems to ensure that all updates to virus software and spyware are installing and scanning regularly. This audit will also ensure all application and operating system security patches are up to date.

Firewalls

By default, any traffic initiated from the outside of the network is blocked. All firewall requests are to be made in writing or via email. Firewall requests must be reviewed by the Technology Director. Traffic originating from the inside is allowed, with some restrictions. SCA uses Lightspeed's Campus Collaboration Bundle to filter internet access to Children's Internet Protection Act (CIPA) standards. The Technology Director can add and remove blocked web addresses at his/her discretion. All requests to allow a blocked site will be directed to the Technology Director.

Remote Access

Do not use automatic saving of passwords on the iPads or any PC that accesses school computers.
Additionally, the logmein account password and domain passwords should be different.

Last thing you want is an iPad or Laptop to get lost and then the 'finder' to have access to a teacher PC. I'd also research remote wipe capabilities for iPad so you could erase all data if one is lost or stolen.
Use the app called Find My iPad and activate it on Ipad2's within their settings. All iPads to have this installed and have it activated.

http://www.apple.com/ipad/built-in-apps/find-my-ipad.html

Require all iPads to have a passcode for access. I'd recommend only Level 3 data be stored directly on them.

Backup of Data

SCA uses a secure vendor for the storage and indexing of system backup data. Backup of Faculty/Staff profiles and shared folders is executed each evening. Student personal drives are

not backed up. In addition to vendor backup, SCA financial data is backed up to the external vendor server and manually backed up to an encrypted flash drive that is taken off location each evening.

Incident Management

Information Security incidents can be summarized as:

- Theft or loss - of laptop, USB drive, portable hard drive, iPad or sensitive information
- Malicious software (e.g. virus, spyware, malware, etc)
- Unauthorized access to a PC/laptop or any school application (e.g. through personal password becoming known, leaving your workstation unlocked when unattended, etc)
- Unauthorized access to the school building / office (e.g. break in or access to an unlocked and unattended room) which could lead to unauthorized access to the network or theft of equipment

Should an incident occur the user would immediately report the facts to the Technology Director. The Technology Director will arrange for the issue to be promptly investigated. A log of such incidents will be maintained and reviewed periodically to ensure that improvements on the information security policies and procedures can be made. SCA IT will maintain an inventory of all SCA equipment, which will support the recording of loss or theft of any equipment or information.

Policy compliance

Students will sign the computer and internet use agreement (appendix A) at the beginning of each school year.

All faculty/staff will receive Information Security Awareness training and policy review during teacher orientation prior to the beginning of the school year. All faculty/staff will sign an information security policy acknowledgement form at the conclusion of this training.

If any user is found to have breached this policy, they may be subject to investigation under the school’s disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).