TECHNOLOGY RESPONSIBLE USE AGREEMENT

Acceptable Use

The use of an assigned account shall only be for purposes directly related to the student's education and within the educational goals and objectives of SFXS. The student's use shall further conform to the Student Handbook, where applicable. Compliance with these rules and restrictions is each user's sole responsibility.

Some activities are illegal and are expressly forbidden:

- Transmission of any material in violation of federal or state laws is expressly prohibited. This includes, but is not limited to the transmission of copyrighted material, threatening or obscene material, or material protected by trade secrets. This restriction applies to the downloading of various files, which, though copyrighted, may be readily available, such as songs, videos, movies, and other media content.
- Unauthorized duplication of programs. The student shall adhere to all state and federal laws pertaining to copyright, meaning that no program may be duplicated with the express permission of the original creator of said program.
- Hacking (the unauthorized retrieval of data) within or into any network or computer system, even when no harm is intended.

Some activities, which may be legal, are not appropriate:

- Use of the School's technological resources is for school-related business only.
- Use of product advertisement or political lobbying, including lobbying for student body office, is not permitted.

Only educational games deemed appropriate by an instructor or teacher are allowed.

No streaming is allowed without the permission of the IT Coordinator. Streaming takes up limited bandwidth and may prevent others from using the network.

Acceptable Devices

Ereaders are allowed at the teacher's discretion. No Smart Watches are allowed to been worn on campus. Cell phones must remain off and in a student's backpack at all times.

Chromebook 1:1 Program

The use of the term “Chromebook” includes the actual device along with the charger issued by St. Francis Xavier School.

All students receiving a Chromebook are responsible for the Chromebook issued to them. For students in grades 3-5, the Chromebooks are left in the classroom, students in grades 6-8 may take theirs home each day. All Chromebooks are to be returned at the end of each school year and will remain on campus over the summer. Upon returning to school in August, the same Chromebook will be assigned to each student. Upon graduating, 8th-grade students may keep their assigned Chromebooks. If for any reason, a student leaves St. Francis that has been issued a device, the device remains the property of SFX and must be returned.

St. Francis Xavier School will issue a school-owned Chromebook to students upon compliance with the following:

- Completion of Student Orientation Training Session
- Submission of signed Student Handbook Form

Terms of Use of St. Francis Xavier School Technology

- Students may be subject to loss of privileges, disciplinary action, legal action, and parents/guardians may be financially responsible for up to $200 for the replacement or repair of the school-issued Chromebook in the event of intentional damage and/or violation of policies and guidelines as outlined in the Technology Responsible Use Agreement of the Family Handbook. The Teacher and School Administrator will assist in contacting the parents/guardians to discuss device damage/loss information to identify the specific response necessary on a case by case basis.
- Students are required to turn in school-issued Chromebooks upon request from any school staff member.
- Students should notify his/her teacher within 24 hours of accidental damage, loss, or theft of a school-issued Chromebook.
- If a school-issued Chromebook is stolen from an off campus location, parents/guardians are required to file a police report within 48 hours and bring a copy of the report to the Principal’s Office. Parents should also notify their student’s Homeroom teacher in the event of theft.

Parent/Guardian Expectations

● Monitor their child's appropriate Internet use and adherence to Internet guidelines when using their school-issued Chromebook.
● Ensure stolen or damaged Chromebooks are reported within the designated timeframes.

Care of the Chromebook

Transporting

● All Chromebooks are required to be transported in a protective sleeve, case, or backpack provided by the student.
● Do not overfill the bag where your Chromebook is stored. (Pressure on the Chromebook can cause permanent damage to the screen and other components)
● Never leave your Chromebook in a car or in an exposed area where it can be stolen. ● Never leave your Chromebook in unsupervised areas during the school day. They are to be securely locked in a classroom. Chromebooks left unsecured may be confiscated to avoid exposure to theft. ● Chromebook is for students' use only. The sole purpose of the Chromebook is for school work only. ● Do not throw your bag with the Chromebook inside.

LCD Screen

● LCD screens are delicate – they don't like being poked, prodded, pushed, or slammed. ● Never pick up your Chromebook by its screen
● Don't slam the screen closed
● Be gentle when putting your device down
Cleaning the Screen
● Switch off your Chromebook
● Lightly dampen a nonabrasive cloth with water and gently wipe the screen in a circular motion
● Do not directly apply water or cleaner to the screen
● Avoid applying pressure to the screen
Case (Outer Shell) Care
● Use a nonabrasive cloth
● Spray cleaner onto cloth to moisten, but do not spray the Chromebook directly.
● Rub gently
● Students are not to personalize their Chromebooks with stickers, carving, writing, or other means.

Power and AC Adaptor

● Connect your adaptor only to your Chromebook
● Do not trade AC adapter with anyone else
● Do not step on your power cord or place heavy objects on top of it
● Keep your cord away from heavy traffic areas
● When unplugging the power cord, pull on the plug itself rather than the cord
● Do not wrap your cord tightly around the adaptor box
● Be aware of the power savings that come from running your device effectively from the battery after being fully charged.
● Netbooks should be charged nightly so students arrive prepared to use them on battery power as needed throughout the school day.

Keyboard

● Gently brush your keyboard with a clean soft-bristled paintbrush or similar to remove dirt. ● If any key tops are missing or keys are in a damaged state, take your Chromebook to the Technology Department to be repaired immediately.

Student Data & Security

● Students are responsible for all data stored on their Chromebooks. Students are provided unlimited storage in Google Drive.
● Students are responsible for verifying their data has been backed up to Google Drive. This is done via an automated process on the Chromebook while connected to the internet.
The Internet
● The use of devices by students is governed by the Technology Responsible Use Agreement that students and parents agree to for use of technology within the school and district. Parents are also to familiarize themselves with the Technology Responsible Use Agreement to further support their adherence outside of the school environment.
● Any inappropriate use of the internet is unacceptable and is subject to disciplinary action and exclusion from the school networks and resources.
● Appropriate use of the internet service within the school network is closely monitored by a filtering system that blocks inappropriate content. This also applies to the use of devices outside of the school network.

Peripherals

The school will not provide or specifically recommend any additional peripherals as part of the 1 to 1 program. However, parents or students may purchase this outside of the program. Program support and warranty will not apply to peripherals. Peripherals may include devices such as:

- USB backup devices
- Additional batteries
- External hard drives
- Mice or External Keyboards
- Headphones

Temporary Loan for Repair

- Repair Loan devices may be available to students if their device has been submitted for repair under warranty conditions.

Use of Other Electronic Devices

With the permission of the teacher, students may record classes for the purpose of better understanding the material presented. Any such recordings may be used for no other purpose. Students shall not bring devices such as a cellular phone, iPod, iTouch, camera, MP3 player, or other electronic communication or entertainment equipment unless they are needed for an academic class.

Network Account: Data Storage

Each user of the SFXS network shall abide by these policies and procedures and generally accepted rules of user etiquette. Only school related data files shall be allowed on the SFX Google Drive file server. Since all students use the same server, space is limited. Please delete old files and pictures at the beginning and end of each school year.

Email

The school provides students with a Gmail account. A student's email account carries with it many benefits. The account allows you to correspond with teachers, communicate and share files with group members, attach documents to work on at home, and more. These benefits are paired with the responsibility of using your email account appropriately.

The following policies are in place to ensure that this form of communication is used properly. Students who violate these policies, at the very least, will lose email privileges.

The school expects that students are to log in and check their SFXS issued email account on a frequent and consistent basis.

- Student password information shall not be shared.
- Students are responsible for all electronic mail originating from their Google account
- Forgery or attempted forgery of email messages is illegal and prohibited.
- Any unauthorized attempt to read, delete, copy, or modify email of other users is prohibited.
- Users are prohibited from sending unsolicited mass emails.
- All users must adhere to the same standards of conduct for communicating online that is expected in the classroom.

It is the student's responsibility to report any potential misuse of student email to the SFX IT department.

Excessive emailing is not only disruptive and inefficient but also uses up limited space in our system. A policy is in place to prevent the overloading of file space. If retention of specific Email information is desired, a hard copy should be printed.

Given the nature of electronic mail as a public medium, it is critical for students to use appropriate language and monitor message content being mindful that we represent St. Francis Xavier School. There should be no expectation of privacy when using email. The school reserves the right to check all email communication when deemed necessary or appropriate. There will be no support for personal email. This includes personal email to/from your SFX account. This also includes external email systems (Gmail, Yahoo, Cox, etc.).

Mobile Device Management (MDM)

Any devices intended to be used in the classroom are required to be enrolled in the Meraki Systems Manager. Access to the internet and shared network resources will not be permitted unless the device is enrolled.

The purpose of the MDM is to allow remote delegation of school WiFi credentials, authorization of applications and documents owned by the school, and delegation of school Network Resources (e.g. Apple TV AirPlay access or school printers).

In exceptional circumstances, such as suspected violation of school policy or criminal activity, Meraki Systems Manager may be used to monitor certain aspects of data usage, remotely lock the device, and/or wipe all SFXS data from the device. This can only occur at the express authorization of the Principal.

● Any device may be locked out of the school network or remotely wiped of SFXS data if:
● The Student terminates his or her connection with the school
● IT detects a data or policy breach, a virus, or a similar threat to the security of the school's data and technology infrastructure.
● IT detects suspicious data usage, including but not limited to excessive volumes of data download/upload.

Lost or Stolen Device

● In the case that a device is lost or stolen the MDM may be used to locate a student's device and/or remotely lock the device. This service can only be provided at the express authorization of the owner of the device.

Safety and Security

Electronic connection to the Internet and other online systems provides many educational opportunities, it also involves risk.

● Students should never give out names, addresses, or telephone numbers (or anyone else's information) to strangers online or anywhere else.
● Students should never arrange face to face meetings with individuals met solely online. It is very difficult to confirm the real identity of individuals met online and is, therefore, a dangerous practice to undertake.
● Security on any computer system is a high priority because there are multiple users whose work is often the product of many hours of time and effort. Students should never use another individual's account (even if it has been left accessible) or log on to the system as someone other than themselves. If a security problem is identified, students should notify the SFX administration at once. Do not demonstrate the problem to other users.
● Students should never give out their passwords to anyone. Students are solely responsible for their accounts, and improper or illegal activities that occur while someone is logged on to the network under a student's account are their responsibility.
● Electronic equipment, regardless of ownership, (student or School) must never be left unattended outdoors or in public school areas (i.e., the library, commons, gym etc.).

Cyberbullying

All members of the SFXS community are to show respect, acceptance, and concern for others. Cyberbullying, in any form, will NOT be tolerated. This applies to the school's network AND the

broader Internet, whether accessed on-campus or off-campus, either during or after school hours. Cyberbullying includes, but is not limited to, the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another person by digital means (Email messages, instant messages, text messages, etc).

A community member who believes they are the victim of cyberbullying should not erase the offending material from their device or account. They should print a copy of the offending material and immediately report the incident to a school official. All reports of cyberbullying will be investigated fully.

Social Networking

Social networking websites (Facebook, Twitter, Instagram, etc.) MAY NOT be accessed on school property at any time. The names of users who use these and similar social networking sites off campus may be linked to SFXS, so that any site content reflects on the school community. When a user is online, the user is also representing the SFXS community, and the site content may negatively reflect or affect the reputation and wellbeing of SFXS and others. Accordingly, the school retains the right to monitor student use of these sites. Should inappropriate material be discovered, the school will contact the parents and ask for their assistance in addressing the concern to the extent possible. SFXS reserves the right to pursue disciplinary action.

At no time should a student “friend” a member of SFX’s faculty/staff nor should a member of SFX’s faculty/staff “friend” a student on a social networking website. Texting and tweeting with current SFX employees are appropriate ONLY for school business (campus emergencies, coordination of offsite events.) All other communications must be kept to the SFX Email system. Postings on the Internet must not include derogatory images or defamatory remarks about anyone in the SFXS community, or the school itself.

Cell Phones

A student’s cell phone must be turned off and not used while on campus, including the restrooms, unless granted permission by a teacher. Students may utilize cell phones once they have exited campus through the front gate of the school. If a cell phone is used or heard during the school day, the device will be confiscated, parents will be notified, and the student will proceed through the discipline cycle.

In all cases of confiscation, the Administration reserves the right to check for any inappropriate information that may be stored, received, or sent on any student's confiscated communication or electronic device during the school day or any school sponsored event. When deemed necessary, this information will be downloaded and/or printed.

Vandalism

Vandalism is defined as any malicious attempt to harm or destroy the property of SFXS, another user, or any other agencies or networks that are connected to the Internet. In addition to physical damage inflicted to equipment, vandalism includes, but is not limited to, the uploading, downloading, or creation of computer viruses or other programs designed to damage computers attempts to crash computers or networks and attempts to bypass security arrangements and programs.

Consequences for Misuse of Resources

Violations of these standards of technology usage at SFX may result in disciplinary action. If there is clear evidence of abuse or a threat to system response, integrity, or security, a user's files may be inspected by the School. For violations, a user's access to technology may be suspended in addition to detention, probation, suspension, or expulsion from SFXS.

SFX is not responsible for any damage or loss of any personal device or accessory used no matter what the cause. This includes use both during and after-school hours.

There is no insurance coverage available through SFXS, nor the Diocese of Phoenix for the loss of or damage to the student's personal device, and no claim for damage to or loss of the student's device can be made.