ST. FRANCIS XAVIER SCHOOL
ACCEPTABLE USE POLICIES AND PROCEDURES
2014-2015 SCHOOL YEAR

St. Francis Xavier School ("SFXS") has implemented a voluntary **B**ring **Y**our **O**wn **D**evice (BYOD) program. The following policies and rules apply to all users and the proper campus use of personal devices along with those supplied by SFXS. Inappropriate use of any device shall result in the revocation of the student's device and network service privileges along with possible further disciplinary action. Both parent and student, whose signatures appear at the end of the document, agree and understand that the student is solely responsible for the student's personal device while on the St. Francis School and Parish property.

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.

<u>Some activities are illegal and are expressly forbidden</u>:

- 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.

<u>Some activities, which may be legal, are not appropriate</u>:

- Use of the School's technological resources is for school-related business only. The School must first approve any other use.

- 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 permission of the IT Coordinator. Streaming takes up limited bandwidth and prevents others from using the network.

Acceptable Devices

The following devices or categories of device are acceptable:

- E-readers such as Kindles, Nooks, Sony Reader, etc.
- Tablet computers such as iPad, Kindle Fire, Samsung Note or Tab, Microsoft Surface, Google Nexus, etc.

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 3rd – 8th grade 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 sign-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.
- An 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 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, remote installation 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:

1. The Student terminates his or her connection with the school
2. IT detects a data or policy breach, a virus or similar threat to the security of the school's data and technology infrastructure.
3. 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

While 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 password 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.).

Personal Laptop Use

Personal laptop use is allowed. SFXS will not be responsible for personal laptop repairs. The technology department will get those who bring computers on campus onto the SFXS wireless network. All SFXS technology policies apply to personal electronic devices including laptops and cellular laptop cards.

Cyberbullying

All members of the SFXS community are to show respect, acceptance, and concern for others. Cyber bullying 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 cyber bullying 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 cyber bullying 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 well-being 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 off-site 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.

Vandalism

Vandalism is defined as any malicious attempt to harm or destroy 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 SFXS 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.

SFXS is not responsible for any damage or loss of any 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.

ST. FRANCIS XAVIER SCHOOL
ACCEPTABLE USE POLICIES AND PROCEDURES
2015-2016 SCHOOL YEAR

I have read and understand the policies and procedures and agree to use the school computer facilities and any personal devices brought to school within these guidelines. I acknowledge that the St. Francis Xavier School Acceptable Use Policies and Procedures regarding Bring Your Own Device (BYOD) are subject to change over the course of the school year, as we strive to ensure that technology is being utilized in a safe and educational fashion.

Student Name:	Signature/Date
Parent/Guardian Name:	Signature/Date