St. Anthony
School Device Handbook

Students and parents are expected to sign and turn in the Acceptable Use Policy and Loan Agreement Form located on the last page prior to being issued a device.

The policies, procedures, and information within this document apply to all school owned Chromebooks, laptops and iPads used at St. Anthony School by students, staff or guests including any other device considered by the Administration to fall under this policy. Teachers may set additional requirements for Chromebook/iPad use in their classroom.

Revised 12/9/21

St. Anthony School strives to understand that technological advancements are happening at a rapid rate and is committed to preparing students for an ever changing world.

Use of Technology

All students in grades 3 - 8 will be issued a Chromebook for educational use in school. Students in grades K- 2 will be assigned a personal iPad, which, in the event of Distance Learning, can be taken home for school use. This document provides students and their parents/guardians with information about the general use of technology, ownership of the devices, rights and responsibilities for possession of the device, educational use, care of the loaned device and being a good digital citizen.

Students and their parents/guardians are reminded that use of School Technology is a privilege and not a right and that everything done on any school-owned computer, network, or electronic communication device may be monitored by school authorities. Inappropriate use of school technology may result in limited or banned computer use, receiving a failing grade, and/or disciplinary consequences. To understand the technology use expectations, students and their parents/guardians are responsible for reviewing this Handbook of policies.

Ownership of the Chromebook/iPad

St. Anthony School retains sole right of possession of the issued device. The device is on loan to the student for educational purposes for the duration of the school year. These Chromebooks and their accessories cannot be borrowed or lent to someone else. To do so violates the contract between the school and child and may be cause for disciplinary action.

St. Anthony administrative staff and faculty retain the right to collect and/or inspect Chromebooks/iPads at any time, including via electronic remote access and to alter, add or delete installed software or hardware. The school will maintain a log of all Chromebooks/iPads that includes the serial number, asset tag, and name of the student assigned to the device.

Receiving Your Chromebook/iPad

All parents/guardians and students are required to sign the Acceptable Use Policy and Loan Agreement Form before a Chromebook will be issued to the student. Each student will receive a Chromebook/iPad, protective case (if applicable) and power charger.

Returning Your Chromebook/iPad

a. End of the School Year

At the end of the school year, students will turn in their device, protective case (if applicable), and power charger. Failure to turn in a device and accessories will result in the student being charged the full $250.00 replacement cost (Chromebook) or $700.00 replacement cost (iPad). If not paid, a report of stolen property with the local law enforcement agency may be filed by the school or school designee.

b. Transferring / Withdrawing Students

Students who transfer out of or withdraw from Sullivan School District must turn in their device and accessories on their last day of attendance. Failure to turn in the device and accessories will result in the student being charged the full replacement cost (see above). Unpaid fines and fees of students leaving St. Anthony may be turned over to a collection agency. Students with outstanding fees will have their report cards and records placed on hold until the issue is resolved. Additionally, a report of stolen property with the local law enforcement agency may be filed by the school or school designee.

Taking Care of Your Device

Students are responsible for the general care of the device they have been issued by the school. Devices that are broken must be reported as such to the teacher as soon as possible so that they can be taken care of properly. District owned devices should never be taken to an outside computer service for any type of repairs or maintenance.

a. General Precautions

● No open food or drink should be next to devices.
● Cords, cables, and removable storage devices must be inserted carefully into devices.
● Devices should not be used with the power cord plugged in when the cord may be a tripping hazard.
● Devices must remain free of any writing, drawing, stickers, and labels.
● Heavy objects should never be placed on top of devices.

b. Protective Cases (if applicable)

● Each student may be issued a protective case for his/her device that should remain on the device at all times.
● Although the cases are reinforced to help protect the devices, they are not guaranteed to prevent damage. It remains the student’s responsibility to care for and protect his/her device.

c. Carrying Devices

● Always transport devices with care and in the school issued protective cases (if applicable). Failure to do so may result in disciplinary action.
● Never lift Chromebooks by the screen.
● Never carry Chromebooks with the screen open.

d. Screen Care

● The device screen can be damaged if subjected to heavy objects, rough treatment, some cleaning solvents, and other liquids.
● The screens are particularly sensitive to damage from excessive pressure.
● Do not put pressure on the top of a device when it is closed.
● Do not store a Chromebook with the screen open.
● Do not place anything in the protective case (if applicable) that will press against the cover.
● Make sure there is nothing on the Chromebook keyboard before closing the lid (e.g. pens, pencils, or papers).
● Clean the screen with a soft, dry antistatic, or microfiber cloth. Do not use window cleaner or any type of liquid or water on the device. You can also purchase individually packaged pre moistened eyeglass lens cleaning tissues to clean the screen. These are convenient and relatively inexpensive.

e. Asset Tags

● All Chromebooks will be marked with an asset code and school logo that must be visible at all times.
● Asset tags and serial number stickers may not be modified or tampered with in any way.

Grades 3-8
Using Your Chromebook At School

Students are expected to have a fully charged Chromebook at school every day and bring their Chromebooks to all classes unless specifically advised not to do so by their teacher.

a. Chromebooks being repaired

- Students and their parents are responsible for repair or replacement costs for damaged or lost Chromebooks.
- Loaner Chromebooks may be issued (if available) to students when they turn in their Chromebook for repair.
- A student borrowing a Chromebook will be responsible for any damage to or loss of the loaned device, just like it was their original school issued device.
- The loaner Chromebook must be returned when the repaired Chromebook is picked up.

b. Charging Chromebooks

● Students should charge their Chromebooks at school every day.
● A fully charged Chromebook battery should last throughout the entire school day.

c. Backgrounds and Themes

● Inappropriate media may not be used as Chromebook backgrounds or themes.
● No images or graphics containing people can ever be used as a background or theme. The presence of such media will result in disciplinary action.
● St. Anthony School administrative staff have the right to change a background or theme on a Chromebook at any time for any reason.

d. Sound

● Sound must be muted at all times unless permission is obtained from a teacher.
● Headphones may be used at the direction of the teachers.
● Students should purchase their own personal set of headphones for sanitary reasons if they wish to use them with their Chromebook.

e. Printing

● Students will be encouraged to digitally publish and share their work with their teachers and peers when appropriate.
● Students must gain permission before printing from their devices.

f. Logging into a Chromebook

● Students will log into their Chromebooks using only their school issued Google Suite (stanthonyschoolsullivan.com) account.
● Students should never share their account passwords with other students.
● Account passwords may not be changed without permission from the teacher.
● If a student believes their password has been compromised, they can request a password reset.

g. Managing and Saving Your Digital Work With a Chromebook

● Students should always remember to save frequently when working on digital media when working outside of Google Drive.
● The school will not be responsible for the loss of any student work.
● Students are encouraged to maintain backups of their important work by having multiple copies stored in different Internet storage applications.

Protecting & Storing Your Devices

● Under no circumstances should a device be left in unsupervised areas. Unsupervised areas include: the school grounds and campus, the cafeteria, unlocked classrooms, library, hallways, bathrooms or any other entity that is not securely locked or in which there is not supervision.
● Unsupervised devices will be confiscated by staff and taken to the office.
● Disciplinary action may be taken for leaving a device in an unsupervised location.
● Devices should always be stored in classroom when not in use.

Repairing/Replacing Your Chromebook/iPad

a. Manufacturer Warranty

● Devices include a one year hardware warranty from the manufacturer.
● The manufacturer warrants the device to be free from defects in materials and workmanship.
● The manufacturer warranty covers normal use, mechanical breakdown, and faulty construction. The manufacturer will provide repair to the device inside the scope of this warranty.
● The manufacturer warranty does not warrant against damage caused by misuse, abuse, or accidents.

b. Chromebooks Needing Repair

● All devices in need of repair must be brought to the school as soon as possible.
● If repair is needed due to malicious damage, the school may refuse to provide a loaner device.
● Repaired devices may end up with the original factory image as first received. It is important that students keep their school data synced to the cloud drives so documents and class projects will not be lost.
● Students and parents will be charged for device damage that is a result of misuse, accidents, or abusive handling.
- Costs incurred for repair shall be paid for by the student's parents or guardians. Cost of repair cannot exceed the cost of a new replacement device.

Operating System and Security

● Students may not use or install any operating system on their Chromebook other than the current version of ChromeOS that is supported and managed by the school.
● The Chromebook operating system, ChromeOS, updates itself automatically. Students do not need to manually update their Chromebooks.
● Chromebooks use the principle of "defense in depth" to provide multiple layers of protection against viruses and malware, including data encryption and verified boot.
● There is no need for additional virus protection to be installed on a Chromebook.

Content Filter

The school utilizes an Internet content filter that is in compliance with the federally mandated Children's Internet Protection Act (CIPA). All Chromebooks will have all Internet activity protected and monitored by the school while on campus. If an educationally valuable site is blocked, students should contact their teachers to request the site be unblocked.

Software

● Chromebooks seamlessly integrate with the Google Suite of productivity and collaboration tools. This suite includes Google Docs (word processing), Sheets, Slides, Drawings, and Forms.
● All work is stored real time in the cloud on Google's secure servers. This cloud based storage allows students to access their work anywhere and from any device with internet access.
● Students are allowed to install appropriate Chrome web apps and extensions from the Chrome Web Store to their Chromebook with teacher permission.

● Students are responsible for the web apps and extensions they install on their Chromebooks. Inappropriate material will result in disciplinary action.
● Some web apps will be available to use when the Chromebook is not connected to the Internet.

No Expectation of Privacy

Students have no expectation of confidentiality or privacy with respect to any usage of a Chromebook, regardless of whether that use is for school-related or personal purposes, other than as specifically provided by law. The school may, without prior notice or consent, log, supervise, access, view, monitor, and record use of student Chromebooks at any time for any reason related to the operation of the school. By using a Chromebook, students agree to such access, monitoring, and recording of their use. Teachers, school administrators, and the technology department staff may use monitoring software that allows them to view the screens and activity on student Chromebooks.

Guarding Sensitive Information

One fundamental need for acceptable student and employee use of District electronic resources is respect for, and protection of, password/account code security, as well as restricted databases files, and information banks. Personal passwords/account codes may be created to protect students and employees utilizing electronic resources to conduct research or complete work.

These passwords/account codes shall not be shared with others; nor shall students or employees use another party's password except in the authorized maintenance and monitoring of the network. The maintenance of strict control of passwords/account codes protects employees and students from wrongful accusation of misuse of electronic resources or violation of District policy, state or federal law. Students or employees who misuse electronic resources or who violate laws will be disciplined at a level appropriate to the seriousness of the misuse.

Acceptable Use

The use of the school’s technology and electronic resources is a privilege, which may be revoked at any time. Staff and students are only allowed to conduct electronic network-based activities which are classroom or workplace related. Behaviors which shall result in revocation of access shall include, but will not be limited to: damage to or theft of system hardware or software; alteration of system hardware or software; placement of unlawful information, computer viruses or harmful programs on, or through the computer system; entry into restricted information on systems or network files in violation of password/account code restrictions; violation of other users' rights to privacy; unauthorized disclosure, use or dissemination of personal information regarding minors; using another person's name/password/account to send or receive messages on the network; sending or receiving personal messages on the network; and use of the network for personal gain, commercial purposes, or to engage in political activity.

Students and employees may not claim personal copyright privileges over files, data or materials developed in the scope of their employment, nor may students or employees use copyrighted material without the permission of the copyright holder. The Internet allows access

to a wide variety of media. Even though it is possible to download most of these materials, students and staff shall not create or maintain archival copies of these materials unless the source indicates that the materials are in the public domain.

Access to electronic mail (E-mail) is a privilege and designed to assist students and employees in the acquisition of knowledge and in efficiently communicating with others. The school E-mail system is designed solely for educational and work related purposes. E-mail files are subject to review by Archdiocese and school personnel. Chain letters, "chat rooms" or Multiple User Dimensions (MUDs) are not allowed, with the exception of those bulletin boards or "chat" groups that are created by teachers for specific instructional purposes or employees for specific work related communication.

Students or employees who engage in "hacking" are subject to loss of privileges and the school discipline policy, as well as the enforcement of any Archdiocesan policy, state and/or federal laws that may have been violated. Hacking may be described as the unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems, or programs, or other property of the, a business, or any other governmental agency obtained through unauthorized means.

To the maximum extent permitted by law, students and employees are not permitted to obtain, download, view or otherwise gain access to "inappropriate matter" which includes materials that may be deemed inappropriate to minors, unlawful, abusive, obscene, pornographic, descriptive of destructive devices, or otherwise objectionable under current District policy or legal definitions.

The District and school administration reserves the right to remove files, limit or deny access, and refer staff or students violating the Board policy to appropriate authorities or for other disciplinary action.

Privileges

The use of school technology and electronic resources is a privilege, not a right, and inappropriate use will result in the cancellation of those privileges. All staff members and students who receive a password/account code will participate in an orientation or training regarding proper behavior and use of the network. The password/account code may be suspended or closed upon the finding of user misuse of the technology system or its resources.

Network Etiquette and Privacy

Students and employees are expected to abide by the generally accepted rules of electronic network etiquette. These include, but are not limited to, the following:

System users are expected to be polite. They may not send abusive, insulting, harassing, or threatening messages to others.

System users are expected to use appropriate language; language that uses vulgarities or obscenities, libels others, or uses other inappropriate references is prohibited.

System users may not reveal their personal addresses, their telephone numbers or the addresses or telephone numbers of students, employees, or other individuals during E-mail transmissions.

System users may not use the District's electronic network in such a manner that would damage, disrupt, or prohibit the use of the network by other users.

System users should assume that all communications and information is public when transmitted via the network and may be viewed by other users. The system administrators may access and read email on a random basis.

Use of the District's electronic network for unlawful purposes will not be tolerated and is prohibited.

Services

While the school is providing access to electronic resources, it makes no warranties, whether expressed or implied, for these services. The school may not be held responsible for any damages including loss of data as a result of delays, non-delivery or service interruptions caused by the information system or the user's errors or omissions. The use or distribution of any information that is obtained through the information system is at the user's own risk. The school specifically denies any responsibility for the accuracy of information obtained through Internet services.

Security

The school recognizes that security on the school's electronic network is an extremely high priority. Security poses challenges for collective and individual users. Any intrusion into secure areas by those not permitted such privileges creates a risk for all users of the information system.

The account codes/passwords provided to each user are intended for the exclusive use of that person. Any problems, which arise from the user sharing his/her account code/password, are the responsibility of the account holder. Any misuse may result in the suspension or revocation of account privileges. The use of an account by someone other than the registered holder will be grounds for loss of access privileges to the information system.

Users are required to report immediately any abnormality in the system as soon as they observe it. Abnormalities should be reported to the classroom teacher or system administrator.

The school shall use filtering, blocking or other technology to protect students and staff from accessing internet sites that contain visual depictions that are obscene, child pornography, or harmful to minors. The school shall comply with the applicable provisions of the Children's Internet Protection Act (CIPA).

Vandalism of the Electronic Network or Technology System

Vandalism is defined as any malicious attempt to alter, harm, or destroy equipment or data of another user, the District information service, or the other networks that are connected to the Internet. This includes, but is not limited to, the uploading or the creation of computer viruses, the alteration of data, or the theft of restricted information. Any vandalism of the school electronic network or technology system will result in the immediate loss of computer service, disciplinary action and, if appropriate, referral to law enforcement officials.

Consequences

The consequences for violating the school Acceptable Use Policy include, but are not limited to, one or more of the following:

1. Suspension of District Network privileges;
2. Revocation of Network privileges;
3. Suspension of Internet access;
4. Revocation of Internet access;
5. Suspension of computer access;
6. Revocation of computer access;
7. School suspension;
8. Expulsion; or
9. Employee disciplinary action up to and including dismissal.

ST. ANTHONY CATHOLIC SCHOOL

ACCEPTABLE USE POLICY AND LOAN AGREEMENT FORM

We believe the Internet offers vast, diverse, unique resources to both students and staff. Our goal in providing this service to teachers and students is to promote educational excellence in school by facilitating resource sharing, innovation, and communication.

With access to computers and people all over the world also comes the availability of material that may not be considered to be educational value in the context of the school setting. On a global network it is impossible to control all materials and an industrious user may discover controversial information. We have installed Open DNS to assist with Internet use. However, the software is not entirely effective in blocking access. We encourage you to use this as an opportunity to have a discussion with your child about family values and your expectations about how these values should guide your child's activities while they are on the Internet.

The smooth operation of the network relies upon proper conduct of the end users that must adhere to strict guidelines. The guidelines provided in the St. Anthony School Device Handbook should be followed by each student and staff member. The signatures at the end of this document indicate that the parties who signed have read the terms and conditions carefully and understand their significance.

1. The user of school computers must support educational information consistent with the educational objectives of St. Anthony. Transmission of any material in violation of any U.S.

or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret. Use for commercial activities are generally not acceptable.

2. Each student will be assigned a school gmail account.
Students may **not** use school computers to access any other email accounts. The school gmail account is restricted to use for school related purposes. It may not be used for personal purposes including, but not limited to, signing up for sites or apps to circumvent parental wishes.

3. Student's may not reveal the school's address or phone number without consulting a teacher first.

4. Users are expected to abide by the generally accepted rules of network etiquette as described in the St. Anthony School Device Handbook.

5. Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the internet, you must notify the teacher. Do not demonstrate the problem to other users. Users shall not intentionally seek information on, obtain copies of, or modify files, or other data, or passwords belonging to others, or misrepresent other users on the network. Attempts to gain unauthorized access to system programs or computer equipment will result in cancellation of user privileges.
Downloading of information onto the hard drives is prohibited. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to school computers.

6. **Vandalism will result in cancellation of privileges.** Vandalism is defined as any malicious attempt to harm, modify, or destroy computer hardware, data of another user, internet, or any of the other networks that are connected to the network. This includes, but is not limited to, the uploading or creation of computer viruses.

7. **Inappropriate use:** The system administrators will deem what is inappropriate use and their decision is final. The administration, faculty, and staff at St. Anthony may deny, revoke, or suspend computer use.

8. Students may not use the internet without a teacher present. Student use of the internet will be monitored at all times.