Freire Charter School (FCS) provides students with computer equipment, computer services, the system network, and Internet access, and other technological equipment and resources. FCS has the right to place reasonable restrictions on this privilege.

All access and rights are privileges granted by FCS and students should have no expectation of privacy in the contents of personal files and access. The situation is similar to the rights you have in the privacy of your locker. Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect privacy with regard to any files stored on school or cloud servers. Routine maintenance and monitoring of the FCS system may lead to discovery that this policy, the FCS Code of Conduct, or the law has been violated. In these cases, students will be held accountable to the expectations of the school and the law.

All users agree to abide by applicable federal, state, and local laws and FCS rules when using FCS technology. FCS will not assume legal or other responsibility for any use deemed unacceptable or for any content students find online.

The use of FCS technology is a privilege, not a right, and the purpose of this agreement is to define acceptable and unacceptable use of computer equipment, computer services, the system network, and the Internet, and other technological equipment and resources as defined by FCS. Unacceptable use, as defined by this agreement, or at the discretion of School staff, may result in restriction or cancellation of access (even for required coursework) as well as other disciplinary or legal action.

PROCEDURE 208A: STUDENT TECHNOLOGY

Technology resources are defined as any electronic tool, device, program, or system that aids the academic environment for a student. Technology includes:

- All computer software and hardware including student chromebooks
- Cell phones, tablets, and smart watches
- Analog and digital networks (e.g., data, video, audio, voice, and multimedia)
- Email systems and communications technologies
- Administrative systems, media systems, and learning information systems
- Smart Boards
- Related and forthcoming systems and new technologies

ACCEPTABLE USE

Acceptable use of the School's technology is any use that is consistent with the educational objectives of the School and in accordance with the Code of Conduct. This includes academic work, college exploration and research, and employment exploration and research. For further clarification on uses not listed here, please refer to the Technology Director. All use is subject to review by the School's staff

Students are responsible for good behavior on school computer networks just as they are on school grounds and in the community. Communications on the network are often public in nature and general school rules apply. Students must respect the rights of others in both the school community and in the global community.

UNACCEPTABLE USE

These rules provide general guidelines and examples of prohibited uses for illustrative purposes but do not attempt to state all required or prohibited activities by students. General examples of unacceptable uses which are expressly prohibited include but are not limited to the following:

- **Illegal Activity** – It is unacceptable use to promote or engage in any activities which are deemed criminal under federal, state or local laws.
- **Copyright Laws** – It is a violation of copyright laws to copy, distribute, display, exhibit, or perform copyrighted works without authority of the owner of the copyright. A copyright notice is not required.

    - Students may not utilize peer-to-peer file-sharing applications or execute programs to facilitate the downloading or exchange of copyrighted or unauthorized music, movies, and other intellectual property, etc.
    - Students may not use the FCS network to arrange for the purchase of illegal substances or alcohol, engage in criminal activity, or threaten the safety of any person(s).
- **Plagiarism** – Students may not plagiarize works that they find on the Internet or other resources (including content generated from artificial intelligence systems).
- **Vandalism** – It is unacceptable use to harm or destroy the hardware, software or data of another user, whether at FCS or at any site connected to the Internet. This includes, but is not limited to, the creation or spreading of computer viruses. If a student breaks a piece of equipment while using it, the family of the student is responsible for replacing that equipment.
- **Security** – Under no conditions should you provide your password to another person. Users are responsible for the security of their account. Users may be held accountable for actions performed under their account name if it has been determined that their account was negligently left accessible. It is also unacceptable to change individual or system passwords. If a user suspects their account security has been compromised they are required to immediately contact an administrator. It is unacceptable to trespass in others' folders, work, or files or to use or to attempt to use another's account, including the System Administrators' accounts. It is unacceptable to post information that could cause damage or a danger of disruption.
- **Offensive Behavior and Harassmen**t – It is unacceptable use to harass, insult, or attack others. It is unacceptable to send or receive any data, which is offensive and/or obscene according to the Code of Conduct. Note that the School may consider an action to be harassment regardless of whether it is considered harassment under the law. Any repeated or unwanted communication may constitute harassment. Any communication with the direct intention of harassing, threatening, implying, or otherwise causing harm to individuals and classes of individuals is a violation of school policy. Be sure to save copies of all harassing material. Provide hard copies to the administration. Harassment is taken very seriously at the School, and anyone who makes false accusations will be penalized. Kinds of Harassment include:
    - Sending/forwarding unsolicited email, junk mail, or propagating chain letters.
    - Email "bombing," spamming, etc.
    - Inappropriate images, text, audio, commentary, etc. that demeans based on ethnicity, race, religion, sexuality, sexual orientation, age, class, disability, etc.
    - Forging electronic information.
    - Creating, altering, or deleting the attribution of origin ("from" in email, IP address headers, etc.).
    - Sending messages under someone else's address or posing as another user in any way.
- **Respect for Resource Limits** – It is unacceptable to intentionally waste limited computer resources. It is unacceptable to download large files. It is unacceptable to post or forward chain letters, send "bomb" emails, or engage in "spamming." Sending numerous or large email messages to one person is considered "email bombing." Spamming is sending an annoying or unnecessary message to a large number of people.
- **Respect for Privacy** – It is unacceptable to repost a message that was sent to you privately without permission of the person who sent you the message. It is unacceptable to post private information about another person.
- **Personal Safety** – It is unacceptable to post personal contact information about yourself or other people. Personal contact information includes your address, telephone, work address, etc. It is unacceptable to agree to meet with someone you have met online for non-academic reasons. This is subject to review by the administration.
- **Commercial Use** – It is unacceptable to offer, provide, or purchase products or services through FCS.
- System Tampering – Any unauthorized alteration of operating systems, individual accounts, software, networking facilities, and/or other programs.
- **Obscenity** – Students may not use the network to access material that is profane or obscene. This includes pornography, inappropriate music or text, etc.

INAPPROPRIATE CONTENT

The policy above states that students may not access any obscene or inappropriate content, that students should have no expectation of privacy, and that system monitoring may lead to the school discovering violations. Freire takes this issue extremely seriously and will issue consequences for violations.

Students are monitored by a service such as Gaggle, which uses technology and trained professionals evaluate content 24 hours a day for potentially harmful content, messages, documents, images and more. If there is discovery of objectionable content or a potentially harmful situation, the monitoring service alerts the school. Programs such as Gaggle are also required by federal law to report suspected child pornography to the National Center for Missing and Exploited Children.

If Freire's automated monitoring system discovers that a student has accessed, stored or sent sexually explicit or inappropriate images, the school will impose discipline and parents and law enforcement will be notified if the School suspects the student has committed a crime.

CHROMEBOOK USE

Freire Schools students have access to Chromebooks. This allows students to direct their own learning and have a greater reliance on active learning strategies. Students will be able to transfer knowledge across disciplines. The increased access to technology will enhance instruction and provide more achievement opportunities for our students.

Software: Only legally licensed software/applications, media, or other data is permitted on the Chromebook. As this computer is the property of the School, the School has the ability to install and uninstall software at our discretion and remotely. Students may not download software, operating systems, applications, or media (including songs, photos, videos) without a prior approval from an authorized school employee.

Privacy: The Chromebooks provided are the property of the School. The chromebook may be examined or searched at any time at the discretion of the School or its employees.

Neither students nor parents/guardians have any right to privacy of any data saved on the Chromebook or in any network drives. The School has the ability to remotely monitor student activity on this Chromebook and will do so at its discretion. The School will never access the camera when the camera has not been activated by the student.

Furthermore, Electronic mail, network usage, and all stored files shall not be considered confidential and may be monitored at any time to ensure appropriate use. The School cooperates fully with local, state or federal officials in any investigation concerning or relating to violations of computer crime laws, and may give proper authorities access to email, files, and network usage data during the course of an investigation.

Saving Files: Students should not save files on the device. The School will provide students locations to save their school-related work. There should be no assumption that files saved directly to the chromebook will be stored indefinitely. Files saved improperly may be deleted at any time. The School accepts no responsibility for lost files.

Remote Access: For chromebooks approved for off-campus use, students and parents are expected to comply with all requests for remote access by the School or approved employees.The School also has the ability to remotely access the Chromebook for purposes, such as locating a lost device, software or program updates, IT support, etc., and may do so without notice to you or your child.

School Rules: All rules, policies, and procedures of the School that apply to students in/during/or at school apply while using the Chromebook. School administrators may develop additional rules regarding use of the device in the future.

Media Access & Safety: Students will have access to all available forms of electronic media (websites, videos, files, etc.) and communication which are in support of the School's educational goals and objectives. Some media and content have been blocked to better ensure the safety of our students. For chromebooks approved for off-campus use, these filters do not replace the importance of parents/guardians in monitoring student Chromebook usage. Parents are expected to be partners in ensuring students' Internet safety.

Acceptable Use: All acceptable and unacceptable uses of technology outlined in the technology policies apply to student chromebooks.

Personal Use & Use by Others: The Chromebook is intended solely for educational use by the student enrolled in the School Students are not permitted to use the computer for personal use. Family members and others are not permitted to use the chromebook for any reason except for assisting a student with a school-sanctioned activity or assignment. For virtual parent-teacher conferences or other parent-school-family virtual meetings, parent use of the chromebook to participate in such meetings is acceptable.

Login Information: Students must log in only with their provided account information. ***Students may not provide their passwords to others.*** Users may be held accountable for actions performed under their account name if it has been determined that their account was negligently left accessible. If a user suspects their account security has been compromised they are required to immediately contact their school's IT Coordinator for support.

In addition to the technology and chromebook policies outlined above, the following policies apply:

CHROMEBOOK ASSIGNMENT

Whether assigned a Chromebook for the class or for approved off-campus use, students are responsible for its care while it's in their possession. Students should not swap or borrow chromebooks from one another. If a student is found to be in possession of a chromebook that is not assigned to them, the chromebook will be returned to the School. If a student is no longer in possession of their originally assigned chromebook, they will be responsible for paying the fee associated with a lost/missing/stolen chromebook.

FEES

If the following damages or losses occur, the parent/guardian agrees to and is responsible for the following fees for repairs and/or replacements which must be paid according to the schedule determined by the School:

Chromebook Charger	$15
Broken/Cracked Screen or Similar Repairs	$50
Lost/Missing/Stolen Chromebook or Damage Beyond Repair	Replacement Cost of Chromebook (minimum $100, not to exceed $300)

Note: Repeated offenses will result in a more substantial charge (not to exceed $300). Repairs due to defects or other technical issues will not incur charges or fees.

CARE OF CHROMEBOOKS

Students are responsible for the general care of the specific device they have been issued by the school:

- The device must remain free of any writing, drawing, stickers, other than any applied by the School.
- For chromebooks approved for off-campus use, the student has responsibility for keeping the chromebook in their possession and supervision at all times. If the chromebook is lost or stolen, replacement fees will be charged (minimum of $100 and not to exceed $300). Lost, missing, or stolen chromebooks must be reported to IT Support immediately.

BRINGING CHARGED CHROMEBOOK TO SCHOOL

For chromebooks assigned for off-campus use, students are expected to come to school each day with a fully charged chromebook. If the chromebook battery is dead or they forget to bring their chromebook, they WILL NOT receive another chromebook for the day. In rare cases for exceptional circumstances (state testing, etc.) a loaner chromebook may be given at the discretion of authorized school employees. The student takes responsibility for this chromebook and may be charged fees for damage/loss of this chromebook as if it were their original assigned chromebook.

RETURN OF CHROMEBOOKS

For chromebooks assigned for off-campus use, the school reserves the right to require the immediate return of the chromebook at any time. The chromebook must be returned if a student withdraws, whether voluntarily or through expulsion, or graduates. Should you fail to return the device within 30 days of the designated return date or if the device is damaged, you agree to pay up to the replacement cost of the chromebook (minimum $100, not to exceed $300).

EXTERNAL RECORDS SHARING WITH ONLINE PLATFORMS

As with the use of most software and websites, students and parents are agreeing to the terms of use and privacy and data sharing provisions, including those of G Suite, Google Classroom, Zoom, Edmentum (Study Island), IXL, GoGuardian, Gaggle, etc.

You can find the Terms of Service for these platforms below:

- G Suite: https://gsuite.google.com/terms/2013/1/premier_terms.html
- Zoom: https://zoom.us/terms
- Edmentum (Study Island): https://www.edmentum.com/terms-of-use
- IXL: https://www.ixl.com/termsofservice
- GoGuardian: https://www.goguardian.com/eula/
- Gaggle: https://cdn.gaggle.net/termsofservice.html

If you have any questions or concerns, please contact your IT Coordinator.

ZOOM EXPECTATIONS

All participants will be held to the following expectations during Zoom sessions:

- Participants will use appropriate language (no cursing, no derogatory language, no disrespect or yelling) during Zoom sessions.
- Participants will mute themselves when they are not speaking to limit background noise.
- Participants will be a positive contributor during the online environment.
- Participants should dress appropriately during the session i.e. no revealing or obscene clothing.
- Participants may not use personalized backgrounds; they may distract from learning.
- The chat feature in Zoom should be used appropriately and be focused on academic conversations. The teacher may disable this feature at their discretion.
- Participants will not be allowed to screen share unless given permission by Freire staff.
- Participants may not edit the shared screen of any zoom participant.

Please be advised that Zoom sessions may serve as a virtual classroom at times. All rules from your physical classroom inside of the school building still apply to the virtual, at home classroom. Inappropriate language, defiance, disruption, and disrespect will and can result in removal from the Zoom learning experience. The Code of Conduct applies to students any time during the Zoom call, whether it be on video or in the 'chat'. If a student is removed from the Zoom learning space, they will be required to meet virtually with either a Dean or a member from the Admin Team before reintegrating into the Zoom. If the behavior continues, the student will be removed from the Zoom session for the remainder of the day and will have a follow-up conversation with their parents and guardians. At that time, it will be determined how the student can be best supported moving forward and reintegrated into future Zoom Session.

We are fully confident that our students will continue to breathe FIRE and uphold the Freire way in this new virtual setting. Please remember that we are a community that supports and lifts one another. Maintaining a safe and productive Zoom classroom is paramount to student success.

Please be aware that as with most software and websites, you are agreeing to Zoom’s terms of use, including their privacy and data sharing provisions.

RECORDING OF STUDENTS

By having your student participate in audio/visual virtual learning or in-classroom learning where a teacher may be recording for virtual learning students, you give consent for their likeness, voice, and statements to be recorded as needed for educational purposes. Participation constitutes your consent under any applicable privacy laws, including the Pennsylvania Wiretap Act (18 Pa.C.S. 5703).

BOARD POLICY 208B: STUDENT USE OF CELL PHONES AND ELECTRONICS

Freire recognizes the importance of communication and collaboration and provides devices for students to be productive in the classroom. To keep the focus on academics and to reduce unnecessary distractions, the Head of School is authorized to develop a system of procedures and consequences related to topics including, but not limited to cell phone use. See below for the School's Cell Phone & Electronics Procedures.

Phones and **personal electronics are not to be used during school. This includes but is not limited to cellphones, smart watches, personal laptops, Meta Glasses, headphones, cameras.** Every student is assigned a personal Yondr Pouch. While the **Yondr Pouch is considered school property**, it is each student's responsibility to bring their assigned Pouch with them to school every day and keep it in good condition (no damages, including bent pin). **Any items put in the pouch other than their working electronics, those items will be confiscated and not returned. S**tudents may be subject to Probationary Contract for Electronics Infractions.

PROCEDURE 208B: STUDENT CELL PHONES & ELECTRONICS

Phones and personal electronics are not to be used during school. Every student is assigned a personal Yondr Pouch. While the **Yondr Pouch is considered school property**, it is each student's responsibility to bring their Pouch with them to school every day and keep it in good condition (no damages, including bent pin). Any items put in the pouch other than their phone, those items will be confiscated and not returned. Students may be subject to Probationary Contract for Electronics Infractions.

DAILY PROCESS

As students Arrive to School and before proceeding to classrooms they will:

1. Turn their personal electronics off.
2. Place their phone (and smartwatches) inside their Pouch and secure it in front of school staff.
3. Store their Pouch in their backpack for the day.

At the end of the day, or if a student is permitted to leave campus for lunch, students will open their Pouch, remove their phone, close their Pouch and put it in their backpack. Students must bring their Pouch to school with them each day. Upon reentering the school building, the cell phone must again be pouched.

*Students arriving late or leaving early will pouch/unpouch their phones in the Main Office.

LEAVING CAMPUS AT LUNCH (HIGH SCHOOL ONLY)

If a student is eligible to leave campus for lunch, they are able to unlock their pouch and retrieve their phone (s) and/or SmartWatch for use outside of the building only. Upon return from lunch, students have to ‘’repouch’’ their phone (s) and/or SmartWatch in the presence of a staff member, similar to the process of arriving to school at the beginning of the day.

POUCH DAMAGE / LOST POUCH / USING PHONE DURING SCHOOL

If a student damages their Pouch or is caught on their phone, Administration will collect the phone/Pouch and call home for:

- The Parent to come to the school and Pick Up their student's phone or the phone may be confiscated overnight
- Additional Consequences may include: Community Service / In-School Suspension / Detention

Examples of damage:

- Ripped
- Cut
- Torn
- Pen/pencil marks
- Bent/cut pin
- Signs of force to black button on flap

FORGOTTEN POUCH

If a student forgets their Pouch, their phone will be collected and Admin will call home to remind the Parent of the policy. The phone will be returned to the student at dismissal. If a student reports to school without a pouch for consecutive days (3 or more), they will automatically be charged for a pouch ($30) and may lose lunch privileges.

If a student consistently forgets their Pouch, it is considered lost and the student will need to purchase another pouch for $30.

If a student loses or damages the pouch the student will need to purchase another pouch for $30.

VIOLATIONS

If any type of electronic device (phone, smart watch, headphones, etc.) is being used without authorization during the school day, the following consequences will be issues:

- First Offense: The staff member will take the phone and it will be returned at the end of the day. The incident will be written up as a CONSEQUENCE - detention will be issued. If the student does not comply or is defiant, there will be additional consequences such as suspension.
- Second Offense: The staff member will take the phone and a parent or guardian will need to retrieve the phone. The incident will be written up as a CONSEQUENCE - detention will be issued, loss of lunch privilege for a week. If the student does not comply or is defiant, there will be additional consequences such as suspension.
- Third Offense: The staff member will take the phone and a parent or guardian will need to retrieve the phone. The incident will be written up as a CONSEQUENCE - The student is put on a phone contract. The length of a phone contract can vary. Students will need to turn in their phone(s) to a Dean at the start of the day and can only get it back after dismissal. If the student does not comply or is defiant, there will be additional consequences such as suspension.

- Fourth Offense: Violation of their Electronics Contract- Suspension issued. The phone will be confiscated and will not be returned to anyone other than a parent/guardian at the informal hearing. Recommendation for expulsion.

Refusal to surrender a requested cell phone or removing the SIM chip from the phone will be considered an act of extreme defiance and will result in the following actions:

- The student's parent will be contacted immediately
- The student will be suspended
- A mandatory informal hearing will be held the next school day
- During this hearing the parent and student will be warned future behaviors like this may lead to more severe consequences
- One (or more) of the following consequences will be assigned:
    - Contract
    - Loss of school privileges
    - Loss of student trips/events
    - Community service

Freire Charter School is not financially responsible for property that a student voluntarily brings to school, including cell phones and other electronic devices, including in the event that property is lost, misplaced, or stolen. Although the school takes every precaution to store confiscated student electronic devices safely and securely, **Freire is not financially responsible for student electronic devices whether they are in the student's or the school's possession**.