Florence 1 Schools
Students first

Florence 1 Schools Device Guide

2023-2024

Table of Contents

Introduction

The mission of Florence 1 Schools is Students first

Florence 1 Schools believes that technology is a powerful tool for transforming learning. It is our vision that all students have access to high-quality interactive educational tools and resources along with high speed connectivity so that learning is everywhere, all the time. Florence 1 seeks to provide learners with engaging and empowering learning experiences that prepare them to be active, creative, collaborative and knowledgeable participants in our globally connected world. We envision that our students will acquire the knowledge, skills and competencies they need to be successful in life and work in the 21st century.

In support of this vision, Florence 1 Schools believes:

- All students must have equitable access to high quality learning experiences transformed by technology, making everywhere, all-the-time learning possible.
- Technology reimagines learning experiences and creates interactive learning environments where students have opportunities to develop critical thinking skills, effectively communicate with others, and build creativity.
- Technology provides unique opportunities for active learning where the teacher becomes the facilitator of knowledge and the student becomes a self-directed and engaged learner.
- Technology can personalize learning and give students more choice over what and how they learn and at what pace, preparing them to organize and direct their own learning for the rest of their lives.

The mission of the Florence 1 Schools digital initiative is to expand and enrich the curriculum with engaged, transformed digital environments that allow students to communicate, collaborate, create, connect, and access information and experts beyond the walls of the classroom. Students will have opportunities for limitless learning, enabling them to be self-directed, responsible, lifelong learners and digital citizens. In order to reach the goal of preparing all learners for the ever-changing tomorrow, this initiative will provide students with digital devices equipped with school-based internet access and Google Workspace for Education, ensuring equitable and functional access to technology.

Use of Technology

The following handbook provides students and their parents/guardians with information about the general use of technology, “ownership”, rights and responsibilities for possession of the digital device, and care of the digital device. All students and their respective parents/guardians must agree to all policies listed in this handbook in order to receive and utilize a digital device, school network, and all other district owned technology-related items. With this privilege and the extraordinary opportunity to explore digital resources, come responsibilities for each student and his/her parents/guardians. Florence 1 will ensure that all students use the digital device and its access to other resources as an essential part of their learning experiences. Along with the efforts of parents/guardians, Florence 1 will follow its policies in maintaining an environment that promotes ethical and responsible conduct in all electronic resource activities and uses.

Ownership

Florence 1 retains sole right of possession and ownership of the digital device and grants permission to the student to use the device according to the rules and guidelines set forth in this document. Florence 1 lends the device to the student only for educational purposes during the academic year. Failure to follow the terms of the policies will result in disciplinary action, including but not limited to, confiscation of any and all devices and accessories lent to the student and revocation of student access to Florence 1 technology, as well as any other disciplinary action deemed appropriate by Florence 1 policy. Florence 1 reserves the right to monitor and log users' (students') use of the district's technology and network and to examine user (student) files and materials as necessary. Moreover, Florence 1 administrative staff retains the right to collect and/or inspect the device at any time, including via electronic remote access; and to alter, add, or delete installed software or hardware. There is no reasonable expectation of privacy while using Florence 1 computers, networks, or technology.

Warranty

All Chromebook devices are covered by a 3-year accidental damage protection warranty (from date of purchase). The protection warranty ONLY covers the Chromebook device; protective cases and power cords are not covered. This protection warranty covers normal use, mechanical breakdown, or accidental damage and will include the provision of replacement parts necessary to repair the device. The warranty does not cover theft, loss, fire, negligence, or intentional damage.

Lost or Stolen Equipment

If any equipment is lost, the student or parent/guardian must report the loss to the school within 48 hours. The circumstances of each situation involving lost equipment will be investigated individually. Parent/Guardian will be billed for lost equipment. Please refer to the User Misuse and Abuse section for replacement costs. The district will not be obligated to replace a student device in the case of negligence and failure to use diligence with district property.

If the equipment is stolen, a police report must be filed and a copy of the report that lists the stolen device must be provided to the school by the student or parent/guardian in a timely manner. The student and parent/guardian will be responsible for the full cost of replacement.

User Misuse and Abuse

Students will be responsible for the entire cost of replacement or repair of the digital device damaged through misuse, neglect, abuse, or intentional damage. If the device is misused or abused, it could be deemed not covered by accidental damage protection. Repair/replacement costs may be charged to the student. Incidents of negligence or repeated incidents become the financial responsibility of the family, up to the full replacement cost of the device. The repair costs below may be applied:

iPad Estimated Repair Cost Due to Deliberate Damage or Neglect:

- Broken screen – $160
- Power adapter - $19; Power cable - $19
- Damaged rear casing – $250
- Full replacement iPad (includes charging cable, warranty) - $378
- Plus Applicable 8% Sales Tax

Chromebook Estimated Repair Cost Due to Deliberate Damage or Neglect:

- Chrome x360 Touch Broken Screen - $150
- Chrome 14 and 11 Touch Broken Screen - $125
- Chromebook 14 & 11 Broken Screen - $100
- Keyboard/Top Cover - $60
- Screen Bezel - $30
- AC Adapter with Power Cord - $45
- Battery - $100
- Hinge - $20
- LCD Back Cover - $35
- Base Enclosure - $45
- Device MAX Case - $32
- Full replacement Chromebook (includes charging cable, warranty) Chromebook 14 Touch $365, Chromebook 14: $335; Chromebook 11: $290; Chromebook 11 Touch: $330; Chromebook x360: $440
- Plus Applicable 8% Sales Tax

Other District Device Repair/Replacement Cost

- Cellular Mifi: $249.99
- Plus Applicable 8% Sales Tax

Distribution of the Florence 1 Digital Device

Before the Florence 1 digital device can be issued, a copy of the Florence 1 Digital Device Agreement and the Florence 1 AUP must be signed by a parent and the student. Each student will be issued a device, a protective case, and power adapter with cord. Devices will be issued to students following an orientation that includes expectations for students and digital citizenship.

Each student's device will be labeled in the manner specified by the district. The digital device can be identified by serial number and the Florence 1 inventory label. The district inventory label and any manufacturer's label should not be removed from the device.

Collection of the Florence 1 Digital Device

The student's device and accessories must be returned during a device check-in day, which will be set by the school, for maintenance over the summer. If a student transfers out of or leaves the district during the school year for any reason (moving, expulsion, early graduation, etc.) during the school year must return the device, including power cords and any other district-issued or school- issued accessories, before leaving the school. All items must be returned with only normal wear and no alterations. Cords and accessories should be maintained and returned in working order. Failure to return items may result in the device being reported stolen and police involvement to recover the device.

Student Responsibilities

The rules and regulations are provided here so that students and parents/guardians are aware of the responsibilities students accept when they use a district-owned device. In general, use of technology requires efficient, ethical, and legal utilization of all digital resources. Violations of these rules and guidelines will result in disciplinary action.

The student will assume responsibility for…

1. Bringing the Device to School

- Unless designated as "day users," or the classroom set model, students must bring devices to school every day that classes are in session.
- Students are responsible for ensuring their device is charged prior to school each day. Students who leave their device at home may be issued another device for that day. However, repeated instances of leaving the device at home may result in no loaner device. In those cases, students will be responsible for all missed activities and assignments due to lack of a device.
- The District will allow headphones and a USB optical mouse to be used while at school. Students who choose to bring any personal accessories such as a wireless mouse or earbuds are aware the district assumes no responsibility in the provision or maintenance of these personal devices.

2. Carrying Device in a Safe and Secure Manner

- Always transport the device in the MAX case provided by Florence 1.
- Always transport device with care and with the screen closed.
- Never lift a device by the screen.

3. Device Security

- Under no circumstances should devices or accessories be left in unsupervised areas. Unsupervised areas include the bathrooms, buses, cafeteria, computer labs, hallways, Library/Media Center, unlocked classrooms, unlocked locker rooms, or any other area deemed insecure. Any device left in these areas is in danger of being stolen or tampered with by unauthorized individuals.

4. General Care

- Never leave the device unattended.

- Never loan the device or its accessories to another student.
- Never set books or stacking heavy objects on top of the device.
- Never set food or drink next to the device.
- Never leave the device exposed to direct sunlight, extreme temperatures, or moisture sources for extended periods of time.
- Only utilize the F1S issued charger for the device.
- Always carefully insert cords, cables, and removable storage into the device.
- Never deface the device and its accessories through use of writing, drawing, stickers, labels, or by any other means.

5. 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, heat, and light. The student is responsible for ensuring the following screen precautions:

- Never put pressure on the top of a device when it is closed.
- Never store a device with the screen open.
- Always make sure there is nothing on the keyboard before closing the lid (e.g. pens, pencils, or disks).
- Only clean the screen with a soft, dry microfiber cloth or anti-static cloth.

6. Device Problems/Repair

If the device is not working properly the student needs to take the device to the Media Center during the times designated by each school. If the device cannot be fixed immediately, the student will be issued a loaner device on a temporary basis. All policies listed in this handbook apply to the student during the loaner period. The student is responsible for ensuring the following:

- The student will never attempt to repair or reconfigure the device.
- The student will not attempt to open or tamper with the internal components of the device; nor should the student remove any screws; doing so will render the warranty void.
- The student and parent/guardian will NEVER take district-owned devices to an outside computer service for any type of repairs or maintenance.

7. Asset Tag

An asset tag is a barcode-like sticker placed on the device for inventory and monitoring purposes. All devices will be labeled with an inventory and asset tag. Tags may not be modified or tampered with in any way. A student may be charged up to the full replacement cost of a device for tampering with a school asset tag logo or turning in a device without a school asset tag.

8. Appropriate Classroom and Library Media Center Routines

When at school the student will use the device and/or any of the school's technology equipment strictly for educational purposes. Using the device for recreational use during class time, or while in the Library is prohibited. Students are expected to fully participate in all classroom activities as directed by their teacher. School staff and district technology personnel may inspect the device without warning or probable cause. In addition to the rules and guidelines set in this handbook, students must abide by all rules and guidelines set by the classroom teacher. Violation of this responsibility will result in disciplinary action.

9. Case Procedures

Students will not be permitted to bring to school a case that has been defaced with inappropriate depictions or language. In the event of a lost or stolen or otherwise unusable case, students must purchase the current district standard case through their school.

Student Accessibility

1. Logging into a device
   - The student will log into his/her device using their district issued account.
   - The student will never share account passwords with other students.

2. Managing and Saving Digital Work with a device
   - The majority of student work will be stored in Internet/cloud-based applications and can be accessed from any computer with an Internet connection and most mobile Internet devices.
   - Student files are to be stored securely within Google Drive.
   - The student should always remember to save frequently when working on digital media. Not all Google tools/apps automatically update.
   - The school will not be responsible for the loss of any student work.

3. Device Cameras
   - The cameras are to be used for educational purposes only, as determined under the direction of a teacher.
   - The use of cameras in restrooms, locker rooms, or on a bus is strictly prohibited. The Family Educational and Privacy Act (FERPA) is a federal law that affords parents certain rights with respect to privacy and educational records. For this reason, students must obtain permission to publish or make publicly available a photograph or video of any school-related activity.

4. Backgrounds and Themes
   - Inappropriate media may not be used as backgrounds or themes. Presence of guns, weapons, pornographic materials, inappropriate language, alcohol, tobacco, drugs, gang-related symbols, or any other content deemed inappropriate by administration will result in disciplinary actions.

5. Printing
   - Students will be encouraged to digitally publish and share their work with their teachers and peers when appropriate.
   - Because all student work should be stored in an Internet/Cloud application, students will not print directly from their devices at school. Any printing that needs to be done must be accomplished by accessing their Google Accounts in labs or the media center or printing at home.

6. Chrome/Apple Web Apps and Extensions
   - Students may install web apps and extensions on their devices that have been whitelisted by the District. The Technology Department will have the ability to select and push out apps and extensions for students.
   - Some web apps will be available to use when the device is not connected to the Internet.

7. Content Filter
   The district utilizes an Internet content filter that is in compliance with the federally mandated Children's Internet Protection Act (CIPA). All Chromebooks, regardless of physical location, will have all Internet activity filtered by the district. Students are bound by the same guidelines in this document whenever they use their Chromebook outside of school.

Google Workspace For Education

Google Workspace for Education is a suite of secure web-based programs for document creation, collaboration and classroom management tools. Florence 1 Schools will provide students with user accounts for Google Workspace for Education. This service is available through an agreement between Google and Florence 1 Schools. Teachers will be using Google Apps for lessons, assignments, and communication.

Google Workspace for Education will also be available at home, the library, or anywhere with Internet access. School staff will monitor student use at school. Parent/Guardian(s) are responsible for monitoring their child's use of Google Workspace when accessing programs outside of school. Google Workspace for Education runs on an Internet domain owned by the school district and is intended for educational purposes only. Student behavior expectations as outlined in this handbook and District Student Discipline Policy will apply.

Discipline/Violations

The use of any technology is a privilege and not a right. Students are expected to use technologies in accordance with classroom rules, guidelines in this handbook, and any applicable local, state, and federal laws. Students are expected to follow all copyright laws pertaining to all media, including text, images, programs, music, and video. Downloading, sharing, and posting online illegally obtained media is against the Acceptable Use Policy. Inappropriate use and violations of these policies will result in disciplinary action and/or repossession of the device and its accessories. In compliance with the Children's Internet Protection Act (CIPA), Florence 1 Schools filters all content for users connected to the internet. Administration may also refer the matter to law enforcement if the violation involves an illegal activity.

System users do not have any expectation of privacy on the contents of their personal files on the district system. An individual search will be conducted if there is suspicion that the user has violated the law or the school disciplinary code. The investigation will be in the context of the nature of the alleged violation. The district will cooperate fully with local, state, or federal officials in any investigation concerning or related to any illegal activities.
(See Appendix C)

Parent/Guardian Responsibilities

Florence 1 Schools provides guidelines to equip parents/guardians with the necessary information to ensure safe use of the devices in the home and community. These are responsibilities assumed by the parent/guardian, which are outlined below:

1. Sign the *Student and Parent/Guardian Digital Device Agreement*
   In order for students to be issued a Chromebook, a student and his/her respective parent/guardian must sign the Student and Parent/Guardian Digital Device Agreement.

2. Accept Liability
   The parent/guardian and student are responsible for the cost of repair or replacement at the date of loss if the property is any of the following:
   - Not returned
   - Intentionally damaged
   - Lost because of negligence
   - Stolen, but not reported to school and/or police in timely manner

3. Monitor Student Use
   The parent/guardian must agree to monitor student use at home and in any setting that is not the school. The best way to keep a student safe and on-task is through parent/guardian presence and continuous involvement, which can be done by completion of the following actions:

   - Investigate and apply parental controls available through the home's Internet service provider and/or wireless router.
   - Develop a set of rules/expectations for Chromebook use at home and in the community.
   - Only allow Chromebook use in common rooms of the home (e.g. living room or kitchen) and not in bedrooms.
   - Demonstrate a genuine interest in what the student is doing on the Chromebook. Ask questions and request they show you his/her work often.

4. Support Internet Safety and Etiquette
   - Internet safety is about helping your child use the Internet productively and practice safe, responsible online behavior. The following are a few basic guidelines to share with your child:
   - Follow your family's rules about when and where to use the Internet.
   - Be polite, kind, and respectful in all digital forums and whenever accessing technology.
   - Understand a website's rules, and know how to flag other users for misbehavior.
   - Recognize "red flags," including someone asking personal questions such as your name and address. Encourage your child to never share his/her name, the school's name, his/her age, his/her phone number, or his/her email or home address with strangers.
   - Never send pictures to strangers.

- Keep passwords private (except from parents, school technology staff, and school administrators).
- Never open a message from a stranger; it may contain a virus that can harm a computer.
- Immediately tell an adult if something makes you feel uncomfortable or is suspicious.
- Visit Common Sense Education Connecting Families (www.commensensemedia.org) which is a website designed to support and empower families in raising kids who think critically, participate responsibly, and behave ethically in their online lives.

Appendix A: Florence 1 Student and Parent/Guardian Digital Device Agreement

Student Agreement:

1. I will take proper care of my digital device.
2. I will not loan my digital device or charger and cords to others.
3. I will be accountable for my digital device at all times.
4. I will charge my digital device's battery as prescribed.
5. I will not leave my digital device in an unsecured location..
6. I will keep food and beverages away from my digital device.
7. I will not disassemble any part of my digital device nor attempt repairs.
8. I will not remove district-required applications.
9. I will not change any district settings or try to bypass content filtering.
10. I will protect my digital device by carrying it in the case provided.
11. I will not stack objects on top of my digital device.
12. I will not leave my digital device outside, or use it near water.
13. I will save school-related data to the district-assigned storage. (Google Drive) Florence 1 will at times Powerwash mobile devices.
14. I will not write or draw on the device; I will not place decorations (such as stickers, markings, sharpie etc.) on my digital device or case.
15. I will not deface the serial number, manufacturer labels or district labels on any digital device.
16. I will follow district policies outlined in the Digital Device Guide and the District's Acceptable Use Policy.
17. I will file a police report in case of theft, vandalism or other violation within 48 hours. I will also notify the school principal within 48 hours.
18. I will be responsible for all damage or loss caused by negligence or abuse.
19. I agree to return my digital device and power cords in good working order.
20. I agree to return my digital device and power cords on the designated date.

Parent/Guardian Agreement:

1. I will be responsible for the repair or replacement costs in the event of loss or damage of the digital device, accessories or case if damage or loss is negligent or deliberate.
2. I will be responsible for monitoring my child's use of the Internet when he/she is not at school.
3. I acknowledge that fraudulent reporting of theft will be turned over to the police to prosecute. I will file a police report in case of theft, vandalism or other violation within 48 hours. I will also notify the school within 48 hours.
4. I agree to immediately return the device and accessories in good working condition upon request.
5. I acknowledge that my student and I are to follow the expectations in the Florence 1 Digital Device Guide, Acceptable Use Policy, and the District's Code of Conduct as outlined in the Student Handbook and that my student is subject to discipline for violation of the expectations outlined in these documents.

Florence 1 Student and Parent/Guardian Digital Device Agreement Signature Page

I have read, understand and agree to the stipulations set forth in the Digital Device Guide, Florence 1 Schools Acceptable Use Policy, and the Student Agreement for Use of the digital device. I understand my digital device is subject to inspection at any time without notice and remains the property of Florence 1 Schools.

Student Name (print) _____ Grade Level _____

Student (signature) _____ Date _____

Parent/Guardian Name (print) _____

Parent/Guardian (signature) _____ Date _____

*__Digital devices__ include District issued devices.

Appendix B: Florence 1 Acceptable Use Policies

Policy IJNDB Use of Technology Resources in Instruction
Issued 1/23

Technology is a vital part of education in the District. For this reason, the District has made arrangements to provide resources to staff and students that promote learning and expand educational resources.

There is a responsibility to use access to the network, Internet, e-mail and other technological services solely for educational purposes and not to access or share inappropriate materials. To that end, the District administration is directed to develop appropriate guidelines governing the use of technology and to implement technology protection measures and safety rules as may be required by the conditions of eligibility for any federal or State technology funding assistance program.

As part of the implementation of the administration's guidelines, students and staff must be instructed on the appropriate use of the network, Internet, e-mail, and other technological services. Students and staff members must also sign a form acknowledging that they have read and understand the Acceptable Use of Technology policy and administrative rule, that they will comply with the policy and rule, and that they understand the consequences of violating the policy or regulations. Inappropriate use of the network, Internet, e-mail or other technological service by any person will not be tolerated, and violations of these guidelines could subject the user to appropriate disciplinary actions, including but not limited to, termination, or removal from the regular school setting.

District and school computer technicians who are working with a computer and come across sexually inappropriate material, including sexually explicit images of children or any other material that could be criminal in nature, must report this to local law enforcement, as well as the appropriate District administrator.

Adopted 12/14/00; Revised 10/11/01, 5/10/12, 1/12/23

Legal References:
United States Code of Laws, as amended:
Children's Internet Protection Act of 2000, 47 U.S.C.A. Section 254(h).
The Digital Millennium Copyright Act of 1998, 17 U.S.C.A. Section 512 - Limitations on liability relating to material online.
S.C. Code of Laws, 1976, as amended:
Section 10-1-205 - Computers in public libraries; regulation of Internet access.
Section 16-3-850 - Encountering child pornography while processing film or working on a computer.
Section 16-15-305 - Disseminating, procuring, or promoting obscenity unlawful; definitions; penalties; obscene material designated contraband.

Policy IJNDB-R Use of Technology Resources in Instruction
Issued 1/23

Access to the network, Internet, e-mail, and other technological services is a privilege, not a right. With this privilege, there also is a responsibility to use these technologies solely for educational purposes and not to access or share inappropriate materials. Inappropriate use by any person will not be tolerated.

I. **Access**

A. General Access

Because technology is a vital part of the educational process and the curriculum of the District, students and staff will be provided access to technology resources. By providing this access, the District intends to promote educational excellence in schools by facilitating resource sharing, innovation, communication, and learning by allowing access to resources unavailable through traditional means. Through the network, Internet, and email students and staff will have access to the following:

- locally networked reference and research sources;
- global information and news;
- discussion groups on a vast range of topics;
- local, regional, public, State, and national library catalogs;
- electronic mail services; and
- online learning and collaboration tools.

The availability of Internet access provides a unique educational opportunity for students and staff to contribute to the District's presence on the Internet. This medium of communication provides an opportunity to share accurate information with the community, our nation, and the world about the District's curriculum and instruction, school-authorized activities, and other related information. The District provides this instructional resource as an educational tool for staff and students, and the technology acceptable use for network, Internet, and e-mail services and administrative rule will govern its use. The failure to follow the policy of this administrative rule may result in the loss of privileges and/or other disciplinary measures.

With access to computers and people all over the world also comes the availability of material that may not be of educational value in the context of the school setting. The District has taken precautions to restrict access to controversial or inappropriate materials; however, on a global network it is impossible to control access to all materials and an industrious user may discover controversial information. The District firmly believes that the valuable information and interaction available on the Internet far outweighs the possibility that users may procure material which is inconsistent with the educational goals of the District. Users are responsible for reporting to the District's Chief Technology Officer, or his/her designee, controversial, or inappropriate websites they are able to access so the websites can be added to the District's filter.

The smooth operation of the network, Internet, and e-mail services relies on the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided so that students and staff are aware of their responsibilities when using these technologies. In general, this requires efficient, ethical, and legal utilization of the network IJNDB-R IJNDB-R 1 of 8 resources.

Because access to the network provides connections to other computer systems located all over the world, users (and parents of students who are users) must understand that neither the District nor any District employee controls the content of the information available on the systems. Every effort will be made by the District to monitor and restrict ready access to known objectionable sites; however, the District does not condone the use of controversial or offensive materials and cannot be held responsible for such use.

B. Technology Protection Measures

In compliance with the Children's Internet Protection Act ("CIPA"), 47 U.S.C. § 254(h), the District uses technological devices designed to filter and block the use of any of the District's computers with Internet access to retrieve or transmit any visual depictions that are obscene, child pornography, or "harmful to minors" as defined in the CIPA. At the same time, the District cannot guarantee that filtering software will in all instances successfully block access to materials deemed

harmful, indecent, offensive, pornographic, or otherwise inappropriate. The use of filtering software does not negate or otherwise affect the obligations of users to abide by the terms of this administrative rule and to refrain from accessing such inappropriate materials. Adult users of a District computer with Internet access may request that the “technology protection measures” be temporarily disabled by the chief building administrator of the building in which the computer is located for bona fide research purposes or other lawful purposes not otherwise inconsistent with this administrative rule. Such requests will be forwarded to the Chief TechnologyOfficer for action.

C. Internet Safety Policy

For purposes of this administrative rule, this is the District’s “Internet safety policy.” This rule includes provisions to address access by minors to inappropriate material on the Internet; the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; to provide for the education of minors about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response; unauthorized access, including so-called “hacking” and other unlawful activities by minors online; unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and measures designed to restrict minors’ access to materials harmful to minors.

D. Responsibilities for Compliance

Prior to accessing the network, Internet, or e-mail services, students and staff will receive instruction on the appropriate use of these services. Students and staff members must sign a form (Exhibits 1 and 2) acknowledging that they have read and understand this administrative rule, that they will comply with the guidelines set forth herein, and that they understand the consequences for violating these guidelines.

II. Terms and Conditions of Use

A. Acceptable Use

The purpose of the District's educational network is to support research and education by providing access to unique resources and the opportunity for collaborative work. All use of the network, Internet, and e-mail services must be in support of education and research IJNDB-R IJNDB-R 2 of 8 and consistent with the educational objectives of the District. Use of other networks or computing resources must comply with the guidelines governing those networks. Transmission of any material in violation of any federal or State laws or regulations is prohibited; this includes, but is not limited to, copyrighted material, materials protected by intellectual property, threatening or obscene material, or material protected by trade secret. Access to computer systems and networks owned or operated by the District imposes certain responsibilities and obligations on users and is subject to District policies and local, State, and federal laws.

Users will use District provided software in a manner that strictly adheres to all licensing provisions, including installation, use, copying, number of simultaneous users, and other terms of the license. Furthermore, users will comply with District policies and follow the District’s best practices where possible to maintain the confidentiality, integrity, and availability of computer systems and information on all devices under their control.

Acceptable use is always ethical, reflects honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and the individual's rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance.

B. Procedures for Use

- Administrators and staff may access the Internet or e-mail for educational or work-related purposes at any time which is not disruptive and does not interfere with the performance of other responsibilities by the employee.
- The District will notify parents/legal guardians about the District network, related safety issues, and issues governing its Internet through a general letter to all parents/guardians. Parental permission is not required for use of the Internet, but parents/legal guardians will be notified that they have the right to file a parent/legal guardian denial form available from the school principal if they do not want their children to have access to Internet resources.
- All computer usage, Internet usage and e-mail usage by District employees and students must be consistent with the District mission and policies.

C. Rules Governing Use of Internet and E-mail

Permitted uses

- Users will utilize the system for educational and professional or career development activities only.
- Users may download text and other non-executable files attached to e-mail messages or from the Internet for school-related business only. Large files should be downloaded during off-peak hours whenever possible.
- Users will check their e-mail frequently and delete unwanted messages promptly. Be aware that the system administrator may delete email at any time.
- Users will subscribe only to high quality discussion group mail lists that are relevant to their educational or professional/career development.

General prohibitions

- Users may not use the District system for commercial purposes, defined as offering or providing goods or services or purchasing goods or services for personal use. The District will not be responsible for any obligations resulting from any unauthorized use of the system.
- Users may not use the system for political activities or to seek to impress or impose personal views on others.
- Users will not post chain letters or engage in spamming. Spamming is sending an unnecessary message to a large number of people.
- Users will not use their email accounts for personal use, with the exception of contacting a family member for emergency, work-related, or school-related purposes.
- Users should not utilize the District e-mail system to advertise or solicit business.
- Users should adhere to common rules for e-mail etiquette.

Personal safety

- Students will not post personal contact information about themselves or other people unless it is in conjunction with a specific teacher-approved assignment or approved college/career communication. Personal contact information includes address, telephone number, school address, etc.
- Students will not agree to meet with someone they have met online without their parent/guardian's approval.
- Students will promptly disclose to an administrator, teacher, or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

Illegal activities

- Users will not attempt to gain unauthorized access to the e-mail system, the District Web pages, or any other computer systems through the District e-mail and/or Internet and/or network access. Users will not attempt to perform functions that exceed their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal.
- Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.
- Users will not use the District system to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of another person, or any other activity that violates existing District policies or procedures. Reference to such activities will not even be made in a joking manner or as a prank.
- The District will notify law enforcement consistent with State law, when potential criminal conduct occurs, as set forth in South Carolina Code Section 59-24-60.

System security

- Users will not share their account information (User ID and/or password) or attempt to log in to another user's account. Any sharing of User ID or password will result in immediate restriction or removal of account privileges. The only potential exception is the sharing of information with IT staff if requested for troubleshooting purposes.
- Users will immediately notify the IT staff if they have identified a possible security problem (students should notify a teacher and/or principal). Do not actively seek security problems but immediately report any potential issues that are found.
- Users will not download or install any unauthorized software or install any unauthorized hardware.
- It is a violation of District policy for employees and/or students to access the Internet within the District using any unfiltered means without prior approval from the Chief TechnologyOfficer. Unfiltered access includes, but is not limited to, Internet access via cellular data providers or use of personal hotspots.
- Users will not knowingly vandalize or cause damage to District equipment or software.
- Users will not knowingly use portable data storage devices which contain viruses or in any other way knowingly spread computer viruses.

Use of appropriate language

Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.

- Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or gang-related language or symbols.
- Users will not post or e-mail information which could cause damage or a danger of disruption of network services.
- Users will not engage in personal attacks, including prejudicial or discriminatory remarks.
- Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending messages, he/she must stop.
- Users will not use any language in an email that threatens another person, whether it is the recipient of the message or a third party.

- Users will not knowingly or recklessly post false or defamatory information about a person or organization.

Access to inappropriate material

- Users will not use the District system to access or send material that is profane, lewd, vulgar, indecent, libelous, or obscene, e.g., pornography that advocates illegal acts or that advocates violence or discrimination towards other people, e.g., hate literature.
- Adult Users who mistakenly access inappropriate information or images should immediately report this to their supervisor. This will initiate proceedings to have the materials blocked.
- Students who mistakenly access inappropriate information or images should immediately report this to the attending teacher. The principal should be notified if it is deemed warranted. This will protect users against an allegation that they have intentionally violated this policy.
- Students are expected to follow parental guidance regarding limitation of access to additional types of inappropriate materials.

Respect for privacy

- Users will not repost or e-mail a message that was sent to them privately without permission from the person who originally sent the message.
- Users will not post or email private information about another person.

Violating software license

- Employees and students are prohibited from participating in any activity that violates such matters as institutional or third party copyright, license agreements, or other contracts. The unauthorized use of and/or copying of software is illegal.
- It is against district practice for employees and students to copy or reproduce any licensed software on district computing equipment, except as expressly permitted by the specific software license. Unauthorized use of software is regarded as a serious matter and any such use is without the consent of the district.

III. Penalties for Improper Use

An employee who violates the terms of this administrative rule or otherwise misuses e-mail or the Internet to access or send inappropriate material will be subject to disciplinary action, up to and including discharge. In addition, the privilege of accessing the Internet and e-mail services also will be subject to cancellation. Students who violate the terms of this administrative rule or who otherwise misuse their access to e-mail or the Internet also will be subject to disciplinary action in accordance with the District Student Behavior Code. Internet access privileges also may be canceled. Violations of the laws of the United States or the State of South Carolina also may subject student or employee users to criminal prosecution. If a user incurs unauthorized costs, the user, as well as the user's parents if the user is a student, will be responsible for all such costs.

Students, parents/legal guardians, teachers, and staff members should be aware that the District may take disciplinary actions for conduct initiated and/or created off-campus involving the inappropriate use of the internet or web-based resources if such conduct poses a threat or substantially interferes with or disrupts the work and discipline of the schools, including discipline for student harassment and bullying.

Any user who deliberately damages District hardware will be charged for any repair or replacement costs. Costs to repair damages that result from deliberate attempts to override or disable protection software will be charged to the user.

IV. Warranty

The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages suffered by any user. This includes loss of data resulting from delays, non-deliveries, misdirected deliveries, or service interruptions caused by the system's negligence, user errors, or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

V. Security

Security on any computer system is a high priority, especially when the system involves many users. If a student or employee believes s/he has identified a security problem on the network, s/he must notify the administrator for the school or the IT Department. Do not demonstrate the problem to other users. Attempts to log on to any network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be subject to severe restrictions, cancellation of privileges, or other disciplinary and/or legal action.

VI. User Privacy

E-mail messages sent or received via a District-issued email account (including home accounts offered through the District) and all other electronic files created using District resources or stored with District resources are property of the District. The District reserves the right to examine, restrict, or remove any material that is on or passes through its network, just as it does any other work or material generated or brought to school by staff or students. Access to electronic information related to any student or staff member will be governed by the same policies that would apply to that information if it were not in electronic form.

VII. School Board Policies

All data housed on the District's resources must conform to Board policies and regulations, as well as established school guidelines. Copies of Board policies are available on the District's website. Persons developing or maintaining web documents are responsible for complying with these and other policies. Some of the relevant issues and related Board policies include the following:

- Electronic transmission of materials is a form of copying. As specified in District policy, no unlawful copies of copyrighted materials may be knowingly produced or transmitted via the District's equipment, including its web server(s).
- Content created for the web and linked to District web pages or social networking sites must meet the criteria for use as an instructional resource in accordance with District policies, regulations, and guidelines.
- Any links on District/school web pages or social networking sites that are not specifically curriculum-related must be approved by the District's Chief TechnologyOfficer. Any other non-curricular materials should be limited to information about other youth activities, agencies, or organizations which are known to be non-sectarian, exclusively devoted to community interests or child welfare, non-profit, and non-discriminatory. Web page links may not include entities whose primary purpose is commercial or political advertising.
- All communications via District web pages or social networking sites will comply with this

policy and the District Student Behavior Code. Offensive behavior that is expressly prohibited by this policy includes religious, racial, and sexual harassment and/or violence.
- Any student information communicated via District web pages or social networking sites must comply with District policies on data privacy and public use of school records.

VIII. Other

1. Material on a web page reflects an individual's thoughts, interests, and activities. Such web pages do not, in any way, represent individual schools or the District, nor are they endorsed or sanctioned by any individual school or the District. Concern about the content of any page(s) created by students or staff should be directed to the building principal of that school.
2. Given the rapid change in technology, some of the technical standards outlined in this regulation may require change throughout the year. Such changes will be made with approval of the Superintendent. This regulation may be updated on an annual basis or more frequently if required.

Florence 1 Schools
Acceptable Use of Technology Resources for Middle and High School Students

Overview
Florence 1 Schools provides access to digital devices, communication systems, the Internet, other digital resources, and new technologies as they become available to support and extend the students' learning experiences. All digital resources used at school or in the performance of school-related activities must be used in a responsible, ethical, and legal manner and in accordance with the policies and educational objectives of Florence 1 Schools. Students must have a signed AUP on file every year and follow the guidelines below which have been established to enhance the learning of individual students while maintaining a safe, functional environment for all. The use of any digital device or any digital resource is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the school district's digital devices or digital resources may result in one or more of the following consequences: suspension or cancellation of use of access privileges; payments for damages and repairs; discipline under other appropriate district policies, including suspension, expulsion, or civil or criminal liability under other applicable laws.

In the event the District is subject to a mandatory closure and implements remote/distance learning, this Policy shall extend to cover the remote/distance learning which occurs virtually utilizing the District's devices and/or accounts. As such, this includes use of video conferencing software and/or live streaming.

Acceptable Uses
At all times, students are expected to:

- Protect login and password information. Only share this information with your parent/legal guardian, school technology staff or school administrator.
- Comply with district guidelines when using assigned third-party accounts for approved digital resources including, but not limited to, Google Workspace for Education, Apex Learning, and Online Textbooks.
- Use school digital devices and Google Workspace for Education apps including email for academic and school-related activities.
- Use the district's electronic communications system, digital devices, and digital resources to communicate in ways that are only kind and respectful.
- Ensure only appropriate content is contained on all digital devices (personal and district) used for student work.
- Alert a school official if unacceptable materials, apps, digital resources are inadvertently accessed.
- Follow copyright and fair use guidelines.

Copyright and Plagiarism
The United States Copyright Law must be followed at all times. Students may not illegally copy text, music, software, pictures, videos or graphics from any Internet, online or software source. The "Fair Use" clause does give students some leniency for using some pictures, music, graphics, text, etc*. for academic purposes only*, and the student's teacher or media specialist will instruct him/her about the legalities and use of this clause when necessary and appropriate. To avoid

allegations of plagiarism, students should always request permission from the creator/owner of material or sites and should cite the digital resource where he/she obtains information or materials.

Privacy
All digital storage, including storage with third party services comes under the direction of Florence 1 Schools. Therefore, the district and technology will review files and communications and monitor online activities. Students should not expect that files stored on district servers or with district-contracted agencies will be private. Network and digital devices and resources are provided as tools for educational purposes only. Florence 1 Schools will employ technology protection measures to ensure data integrity and security.

Students can utilize their webcam to join virtual or onsite class sessions to meet with classes during live sessions or individual teachers. Students can mute their audio and video when needed. All users of these systems have reasonable expectations of privacy.

Unacceptable Uses
The following uses of the school district resources, digital devices, email, apps and digital resources or accounts are considered unacceptable**. At NO time are students permitted to:**

- Use the user names and/or passwords of others or attempt to gain unauthorized access to district resources by any means other than those assigned to the user.
- Access, review, upload, download, store, print, post, distribute, transmit, or receive digital resources that are inappropriate (pornography, hate groups, violence, illegal activity, extremist groups, online advertising, sexting, etc.) to the educational setting or disruptive to the educational process or that could cause damage or danger of disruption.
- Make attempts to degrade or disrupt equipment, software or system performance by intentionally spreading a malicious program or by any other means.
- Use district or non-district hardware, software, network equipment or infrastructure to compromise district network security or disrupt the use of the district resources for other users.
- Use proxies, spyware, or hacking tools to try and get around the district's internet filtering system.
- Engage in any illegal act to violate any local, state or federal statute or law.
- Be disrespectful in emails, postings and comments. No cyber bullying, inappropriate language, personal insults, profanity, spam, racist, sexist or discriminatory remarks, or threatening comments will be tolerated. Any violation of these procedures may result in school disciplinary action.
- Post false or defamatory information about a person or organization, or harass another person, or engage in personal attacks, including bullying, prejudicial or discriminatory attacks.
- Post private information about themselves or another person, unless under the supervision of certified personnel. This includes, but is not limited to, home addresses, telephone numbers, identification numbers, account numbers, access codes or passwords, labeled photographs or other information that would be personally identifiable.
- Access, copy, or download streaming media, music or website resources unless authorized by the instructor for appropriate academic purposes. Users will not distribute unauthorized media content to other users.
- Access chat, game, SMS, social networking, blog or personal email sites or apps except for classroom activities under the direct supervision of certified personnel and with the permission of the FSD1 Technology Director.
- Students will not join a virtual meeting without a staff member present in the meeting OR a staff members approval to be in that meeting.
- Use the district resources or digital devices for unauthorized commercial purposes or for

financial gain, or to purchase goods and services unrelated to the mission of the school district.

Personal Digital Devices

Personal digital devices include, but are not limited to smartphones, laptops, tablets, wearable tech, and eReaders. These are not to be used during class unless the principal and classroom teacher approve its use and the activity is deemed to enhance learning.

1. I understand that my personal digital device can only be used for educational purposes during the school day.
2. I understand that all personal digital devices can only be used during the instructional class period with the express permission of the principal and classroom teacher. This might mean that the device is used for some instructional activities and not others.
3. I will not access personal or social networking apps or sites.
4. I understand my personal digital device may only connect to the F1S Guest Network.
5. I understand that my personal digital device may not contain any inappropriate content.
6. I understand that Florence 1 Schools will not provide any support for my personal digital device at any time.
7. I understand that personal digital devices are brought to school at the owner's risk. Neither F1S nor the school is responsible for theft or damage to the device.

Parent: My signature below certifies I have read the above and agree it is my child's responsibility to follow the guidelines for appropriate and acceptable use.

Parent or Guardian Signature: _____ Date _____

Student: My signature below certifies I have read the above and agree it is my responsibility to use the district's digital devices and digital resources. I assume personal responsibility to behave ethically and responsibly, even when technology provides freedom to do otherwise.

Printed Student Name: _____

Signature of Student _____

Florence 1 Schools

Acceptable Use Policy for Elementary Students

Florence 1 Schools provides a variety of digital devices for educational purposes. These devices include, but are not limited to, computers and laptops; tablets and eReaders; printers and other accessories; drones, robotics and coding devices, and new technologies as they become available. The use of digital devices and online resources is a privilege, not a right. Florence 1 reserves the right to review all network files and to monitor student use of digital devices and digital resources. Students must have a signed AUP on file every year and follow the guidelines below which have been established to enhance the learning of individual students while maintaining a safe, functional environment for all.

In the event the District is subject to a mandatory closure and implements remote/distance learning, this Policy shall extend to cover the remote/distance learning which occurs virtually utilizing the District's devices and/or accounts. As such, this includes use of video conferencing software and/or live streaming.

1. I understand I am assigned an F1S network account that gives me access to F1S Google Workspace for Education. I will only use those accounts and passwords that have been granted by the district for educational purposes at all times.

2. I understand that I may be assigned a third-party account for approved digital resources including, but not limited to, Google Workspace for Education, Dreambox, Discovery Ed, Lexia, apps, and extensions. I will only use those accounts and passwords that have been granted by the district for educational purposes at all times.

3. I will keep my ClassLink badge or username and/or password private and only share with my parents or legal guardian(s). I will not use anyone else's username and/or password to access, send, delete, or change their information including, but not limited to, their files or folders, emails or messages, or data in any digital resources.

4. I will keep my personal information about myself or others private, such as complete name, address, phone number or identifiable picture.

5. I will only use digital devices for educational purposes at all times. I will not access personal or social networking apps or sites.

6. I will communicate in ways that are only kind and respectful to others. I will not create, display, send or share words or pictures that will make someone else angry or upset. I will not use obscene or threatening language. I will not harass, attack, bully or insult others.

7. I will always ask my teacher for permission to download or copy information. I will not download apps, add-ons, extensions, pictures, music, streaming media or copy files that are inappropriate or against district policies.

8. I will get permission and I will give credit for information taken from the Internet. I will not copy information from the Internet, digital resources or other students and turn it in as my work.

9. I will take care of the district's digital devices and networks. I will not damage or change the settings of digital devices, networks and accessories that would cause them to break or to not work.

10. I will report to my teacher any inappropriate digital resources that I access by mistake or that appear on the digital device. I will not use proxies, spyware, or hacking tools to try to get around the school district's Internet filtering system. I will not explore areas of the Internet that are not school related.

11. I will not access chat, games, texts, social networking sites, blogs, and email except for designated classroom activities and under the supervision of my teacher and with the permission of the district technology director.

12. Students will not join a virtual meeting without a staff member present in the meeting OR a staff members approval to be in that meeting.

13. I will not have food or drink when using digital devices.

Privacy

All digital storage, including storage with third party services comes under the direction of Florence 1 Schools. Therefore, the district and technology will review files and communications and monitor online activities. Students should not expect that files stored on district servers or with district-contracted agencies will be private. Network and digital devices and resources are provided as tools for educational purposes only. Florence 1 Schools will employ technology protection measures to ensure data integrity and security.

Students can utilize their webcam to join virtual or onsite class sessions to meet with classes during live sessions or individual teachers. Students can mute their audio and video when needed. All users of these systems have reasonable expectations of privacy.

Personal Digital Devices

Personal digital devices include, but are not limited to smartphones, laptops, tablets, wearable tech, and eReaders. These are not to be used during class unless the principal and classroom teacher approve its use and the activity is deemed to enhance learning.

1. I understand that my personal digital device can only be used for educational purposes during the school day.
2. I understand that all personal digital devices can only be used during the instructional class period with the express permission of the principal and classroom teacher. This might mean that the device is used for some instructional activities and not others.
3. I will not access personal or social networking apps or sites.
4. I understand my personal digital device may only connect to the F1S Guest Network.
5. I understand that my personal digital device may not contain any inappropriate content.
6. I understand that Florence 1 Schools will not provide any support for my personal digital device at any time.

7. I understand that personal digital devices are brought to school at the owner's risk. Neither F1S nor the school is responsible for theft or damage to the device.

Homeroom Teacher Name _____

Parent: My signature below certifies I have read the above and agree it is my child's responsibility to follow the guidelines for appropriate and acceptable use. I understand that F1S provides my student with digital resources for classroom instruction that have been found to meet regulations in regard to the Child Online Privacy Protection Act (COPPA). These tools enhance learning skills such as communication and collaboration, as well as providing the students an opportunity to develop skills that will assist them in lifetime learning skills. Some of these resources may require student login credentials, and I authorize those the District has white-listed.

Printed Name of Parent/Legal Guardian _____

Signature of Parent/Legal Guardian _____ Date _____

Student: My signature below certifies I have read the above and agree it is my responsibility to follow the guidelines for appropriate and acceptable use.

Printed student name (full) _____

Signature of Student _____ Date _____

Appendix C: Florence 1 Digital Device Discipline Plan

Level 1 Violations

Include but are not limited to: repeated uncharged device, unprepared for class, careless or irresponsible use, and off-task behavior.

Level 2 Violations

Repeated Level 1 Violations become a Level 2 Violation.

Level 3 Violations

Include but are not limited to: acceptable use policy violations, photographing/filming others without permission or against their will, bullying with the device, harmful or malicious activities, accessing and/or sharing inappropriate websites, materials, videos or photos.

Level 4 Violations

Include criminal offenses that require the involvement of law enforcement and may require arrest and/or a recommendation for expulsion. Possession and use of personal and/or school issued electronic devices on school property acknowledges consent to search contents of the device in a school or criminal investigation. In such investigations, students will provide necessary login information as needed. Misuse of technology outside of school that impacts the people or environment on campus may also necessitate similar disciplinary consequences and searches.

The administration reserves the right to handle any actions determined to be a misuse of technology in the manner they feel is the most appropriate for all concerned. For additional information on acceptable use of technology, please refer back to the F1S Acceptable Use Policy.