1213 S. 12TH St, Philadelphia, PA 19147 TEL: (215) 400-7970 FAX (215) 400-7971 Principal – Kelly Espinosa

FJC ELEMENTARY COMPUTING AND INTERNET ACCEPTABLE USE POLICY (AUP)

Parents/Guardians, please review this document carefully with your child. The Fanny Jackson Coppin School (FJC) is committed to making your child's technological experiences as safe and meaningful as possible. In order to allow your student access to resources on the School and District's networks as well as the Internet, you must sign the POLICY SIGNATURE PAGE
FORM under the Coppin School Policies & Procedures page on the school's website. This policy will be reviewed with your child in an easy to understand format during computer class. Thank you!

A. Purpose

- 1. FJC provides its students with access to computing equipment such as Chromebooks, network functions such as Intranet and Internet and Email.
- 2. This access is granted for the **sole purpose** of **education** and is to be used to facilitate educational productivity and learning only.
- 3. School Chromebooks are to be used for educational purposes only and for no other reason.

B. Access Rights and Privileges

- 1. FJC has the right to place reasonable restrictions on the use of equipment, resources and materials students access or post through the system. Students are expected to follow the rules set forth in the District's rules and regulations governing conduct, disciplinary code, and the law in their use of District equipment and network. This access has **not** been established as a public access service or a public forum. Access is a **privilege** granted by the District, and Students should expect **NO PRIVACY RIGHTS**.
- 2. All Coppin students will have access to the internet and District provided web-based Gmail through the District's private network. Parents may specifically request that their child/children not be provided such access by notifying the school in writing.

1213 S. 12TH St, Philadelphia, PA 19147 TEL: (215) 400-7970 FAX (215) 400-7971 Principal – Kelly Espinosa

C. Unacceptable Uses

- 1. Students may not use the District's private network or a mobile phone, smartwatch or other electronic device within the school building to purposely access or post material that is obscene, pornographic, profane, or that advocates illegal acts, violence or discrimination towards anyone or any group.
- 2. Students may not write or post personal contact information, images, or recordings about anyone who attends or is affiliated with this school, including themselves, through the school's network or equipment or a mobile phone, smartwatch or other electronic device within the school building. This includes addresses, telephone numbers, school addresses, work addresses, pictures, clips or other identifying information.
- 3. Students may not chat, text or share information, images or posts, about a school community member (on personal or school devices) without the permission of that community member. Doing so is an invasion of their privacy and is not only disrespectful but may cause a considerable disruption to the school community.
- 4. Students may not agree to meet someone they have had contact with through the internet without parental permission and participation.
- 5. Students must login using their authorized SDP Login account and may not attempt to gain unauthorized access to any school or other computer system. This includes logging in as another person, or guest accounts, or trying to gain access to someone else's files. These actions are Illegal, even if for the purposes of "browsing" or "electronic discovery."
- 6. Students may not deliberately disrupt or harm hardware or software systems, interfere with computer or network performance, interfere with another's ability to use equipment or systems, or destroy data. This includes deleting other people's work or purposely unplugging computers, keyboards, mouses or headsets without teacher approval.
- 7. Students may not use the District's "private network" or a mobile phone, smartwatch or other electronic device within the school building to engage in illegal acts, such as arranging for the sale or purchase of drugs or alcohol, engage in criminal gang activity, threaten the safety of another, share unauthorized copyrighted material or intellectual property, etc.
- 8. Students may not use the District's private network or a mobile phone, smartwatch or other electronic device within the school building to solicit information with the intent of using such information to cause harm or injury to another.
- 9. Students may not post information that could endanger another, cause personal damage or a

1213 S. 12TH St, Philadelphia, PA 19147 TEL: (215) 400-7970 FAX (215) 400-7971 Principal – Kelly Espinosa

danger of disruption to service.

- 10. Students may not knowingly or recklessly post false or defamatory information about a person or an organization.
- 11. Students may not intentionally seek information on, obtain copies of, or modify files, data or passwords belonging to other community members.
- 12. Students may not directly or indirectly make connections that create "backdoors" to the District's network which allow unauthorized access to any person or organization.
- 13. Students may not use obscene, profane, lewd, vulgar, rude, inflammatory, hateful, threatening or disrespectful language.
- 15. Students may not engage in personal attacks, including prejudicial or discriminatory attacks.
- 16. Students may not harass or bully another person. Harassment is persistently acting in a manner that distresses or annoys another person. Bullying is unwanted, aggressive behavior among school aged children that involves a real or perceived power imbalance.
- 17. Students may not repost a message that was sent to them privately without the permission of the person who sent them the message.
- 18. Students may not forward or post chain letters, or engage in "spamming." Spamming is sending annoying or unnecessary messages to large groups of people.
- 19. Students will not install or reproduce unauthorized or unlicensed software on SDP resources including downloading extensions to their Chromebook..
- 20. Students may not plagiarize works that they find on the internet or through other sources.
- 19. Students may not use the District's private network for political lobbying.
- 21. Students will not download files unless approved by the teacher.

1213 S. 12TH St, Philadelphia, PA 19147 TEL: (215) 400-7970 FAX (215) 400-7971 Principal – Kelly Espinosa

D. System Security Obligations

- 1. Students are responsible for the use of their individual access account and should take all reasonable precautions to prevent others from being able to use their account. **Under no condition should a user share their password with another person.**
- 2. Any user identified as a security risk or having a history of violating this or any other Acceptable Use Policy shall be denied access to the District's private network and computing equipment for the remainder of the school year.
- 3. Students should immediately notify a teacher or system administrator of any possible security problem or when they have inadvertently accessed inappropriate material or feels that they have been bullied or harassed.
- 4. Students will promptly tell their teacher or other appropriate school employee of any message received that is inappropriate.

E. Filtering

1. As required by law and in recognition of the need to establish a safe and appropriate computing environment, FJC and the District will use filtering technology to prohibit access, to the degree possible, to objectionable or unsuitable content that might otherwise be accessible via the Internet. It is important to recognize that there are approximately 252,000 new websites created worldwide daily and blocking all objectionable material is nearly impossible; however, we will make every effort to ensure that all computer use within the school is carefully monitored.

F. Due Process

- 1. The School District and Fanny Jackson Coppin School will cooperate fully with local, state, or federal officials in any investigation concerning or relating to any illegal activities conducted through the District's private network or from a mobile phone, smartwatch or other electronic device within the school building.
- 2. In the event there is an allegation that a student has violated this Acceptable Use Policy, the student and parent will be provided with notice of the alleged violation and will be afforded the opportunity to be heard in the manner set forth in the Student Hearing Process Policy. Disciplinary actions may be taken.

G. Administration

1. The principal has the responsibility to establish a plan to ensure adequate supervision of students and is also responsible for interpreting and enforcing this policy at the school level.

1213 S. 12TH St, Philadelphia, PA 19147 TEL: (215) 400-7970 FAX (215) 400-7971 Principal – Kelly Espinosa

FJC ELEMENTARY COMPUTING AND INTERNET ACCEPTABLE USE POLICY (AUP)

Signature Page Please Return This Page to School.		
Student: I have read and discussed the	LEMENTARY COMPUTING AND INTERNET ACCEPTABLE USE POLICY (AUP)	
Print Student's Name:		Date:
Student Homeroom #	Grade	
Parent: I have read and understood and discussed with my child the:		
FJC EI	LEMENTARY COMPUTING AND INTERNET ACCEPTABLE USE POLICY (AUP)	
Print Parent 's Name:		
Parent's Signature		Date: