MLA STUDENT CHROMEBOOK TERMS OF USE

Purpose: The Board of Education of the City of Chicago on behalf of Marine Leadership Academy (MLA), will provide computers and network capabilities to MLA students for the purpose of enhancing instruction through technological resources. MLA may make Internet access and/or email on the CPS Network available at school to students as educational resources. It is a general policy of CPS to promote the use of computers in a manner that is responsible and appropriate. Student use of the CPS Network and computer equipment is a privilege. CPS reserves the right to revoke a student's right to use the property and network access in the event that the student fails to adhere to the MLA Student Participation Terms of Use, the CPS Student Acceptable Use of the CPS Network Policy, and the terms of the MLA Consent Form.

Disclaimer: CPS will make a good faith effort to keep the CPS Network system and its available information accurate. Pursuant to the Children's Internet Protection Act, CPS uses filtering software on its network to screen Internet sites for obscene, offensive, and/or sexually explicit material. No filtering software is one hundred percent effective and students accessing the Internet and using email do so at their own risk.

STUDENT USERS ACKNOWLEDGE THAT THERE IS NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, REGARDING THE ACCURACY, QUALITY, OR VALIDITY OF ANY DATA OR INFORMATION AVAILABLE. FOR EXAMPLE, AND WITHOUT LIMITATION, CPS DOES NOT WARRANT THAT THE CPS NETWORK WILL BE ERROR FREE OR FREE OF COMPUTER VIRUSES. IN MAKING USE OF THESE RESOURCES, STUDENT USERS AGREE TO RELEASE THE BOARD FROM ALL CLAIMS OF ANY KIND, INCLUDING CLAIMS FOR DIRECT OR INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY NATURE, ARISING FROM ANY USE OR INABILITY TO USE THE NETWORK, AND FROM ANY CLAIM FOR NEGLIGENCE IN CONNECTION WITH THE OPERATION OF THE CPS NETWORK. STUDENT USERS FURTHER ACKNOWLEDGE THAT THE INFORMATION AVAILABLE THROUGH INTERCONNECTING NETWORKS MAY BE INACCURATE. CPS HAS NO ABILITY TO MAINTAIN SUCH INFORMATION AND HAS NO AUTHORITY OVER THOSE MATERIALS.

CPS MAKES NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, REGARDING THE ACCURACY, QUALITY, OR VALIDITY OF THE DATA AND/OR INFORMATION RESIDING ON OR PASSING THROUGH THE CPS NETWORK FROM OUTSIDE NETWORKS. USE OF THE CPS NETWORK IS AT THE RISK OF THE STUDENT USER. CPS MAKES NO EXPLICIT OR IMPLICT WARRANTY THAT THE FILTERING SOFTWARE USED BY CPS PROVIDES A 100% DETECTION RATE FOR OBSCENE, OFFENSIVE, AND/OR SEXUALLY EXPLICIT MATERIALS. CPS SHALL NOT BE LIABLE FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE FILTERING SOFTWARE TO DETECT OBSCENE, OFFENSIVE, AND/OR SEXUALLY EXPLICIT MATERIAL.

General Information: Students and their families will be responsible for any cost incurred due to lost, stolen or damaged equipment and accessories. The student is responsible, at all times, for proper use of the network and equipment provided to him/her.

CPS NETWORK ACCESS: The Student User of the CPS Network:

- MAY keep a free account on the CPS Network as long as he or she is a student in the Chicago Public Schools;
- MAY use the Internet to research assigned classroom projects;
- MAY use the Internet to send e-mail to other users of the CPS Network and to people around the globe; and
- MAY use the Internet to explore other computer systems.

The Student User of the CPS Network:

- AGREES TO NOT give his or her password to another person;
- AGREES that NONE of his or her communications and information accessible through the CPS Network is considered private or confidential and the Chicago Public Schools reserves the right to access all user accounts, at any time, including student email;
- AGREES to the terms of the CPS Student Acceptable Use of the CPS Network Policy before logging on;
- AGREES that if the CPS Student Acceptable Use of CPS Network Policy is violated, the student's account on the CPS Network will be revoked;
- AGREES that if he or she is removed from the CPS Network by a school faculty member that he or she has the right to appeal the removal within thirty (30) days, in writing, to the principal of the school. The school principal's decision shall be FINAL; and
- AGREES that if he or she is removed from the CPS Network, there shall be no obligation to provide a subsequent opportunity to access the CPS Network, or to provide alternate means of completing required coursework.

COMPUTER OR MOBILE DEVICE USE

The computer or mobile device is an educational tool and shall only be used in that capacity. Once issued, the student and consenting parent or guardian are responsible for the computer or mobile device at all times.

1. MLA/CPS is not responsible for computer or mobile device assigned to students that have been left in the classroom, hallway, or locker.

2. The student is the only authorized user of his/her assigned computer or mobile device. Never share or trade computers or mobile devices with another student.

3. Parents should have access to the student's computer or mobile device, login, and password.

4. Use the computer or mobile device on a flat, stable surface.

5. Never use cleaners such as Windex to clean computer or mobile device screen.

6. Do not mark the computer or mobile device in any way with markers, stickers, or other damaging materials.

7. Do not remove district applied labels, asset tags, or other identifiers.

8. Computers or mobile devices must be brought to school at MLA daily, fully charged and with the power cord.

9. Computers or mobile devices are property of MLA/CPS. If you stop attending MLA, you must return the computer or mobile device to MLA immediately or you will be in possession of stolen property. The Board reserves the right to take legal action in the event you fail to return the property to

MLA. COMPUTER TRANSPORT AND HOME USE

1. Computers are to be protected in the students' school bag or backpack. It is highly recommended that you purchase a case or protective sleeve for transportation to and from school.

2. Never use the computer on public transportation, or before/during/after practices, games, and extracurricular activities.

3. Keep all food and drinks away from the computer.

4. Do not leave the computer in an automobile. Computers cannot tolerate extreme heat or cold and may become damaged.

5. Failing to bring the computer or mobile device to class daily will result in the inability to participate in class work, homework and projects.

PARENTS

1. When the computer is home, it is recommended by CPS that the parent/guardian require the student to use the computer or mobile device in a common room where adult supervision can be maintained at all times.

2. CPS does not provide home access to the Internet.

3. Parents/guardians have the right to their child's login and password in order to facilitate in the supervision of the student's computer usage at home.

4. CPS' content filter is not applied in home settings and parents/guardians accept full responsibility for monitoring their child's Internet use. CPS shall not be responsible for a student obtaining access to inappropriate Internet sites or improper use of the computer or mobile device due to his or her parent/guardian's failure to properly supervise the student's use of the computer or mobile device.

5. If a student returns to school without the assigned computer the parent/guardian will be contacted immediately and agrees to bring the computer or mobile device to school.

6. Replacement costs or repair costs for damages not covered under the manufacturer's warranty that occur to the computer or mobile device and its sleeve while the student participates in the MLA are the sole responsibility of the parent/guardian.

STOLEN OR LOST EQUIPMENT

If the computer or mobile device is stolen, the police must be notified within twenty-four (24) hours of the theft. A police report must be filed and failure to do so will result in the parent/guardian's complete responsibility for the computer's or mobile device's replacement. If the computer or mobile device is stolen or lost, the parent/guardian of the student shall notify the principal or assistant principal of MLA that the computer or mobile device is stolen or lost within twenty-four (24) hours of the loss or theft. In the event that a lost computer or mobile device is not recovered within five (5) business days from the date of the loss, the parent/guardian shall be responsible for the computer's or mobile device's replacement.

IMPROPER USE OF THE CPS NETWORK AND EQUIPMENT

Improper use of the CPS Network is prohibited. Uses of the CPS Network and equipment that are prohibited include, but are not limited to:

1. Use of the CPS Network or equipment for, or in support of, any ILLEGAL purposes;

2. Use of the CPS Network or equipment for, or in support of, any OBSCENE or PORNOGRAPHIC purposes; this includes, but is not limited to, the RETRIEVING or VIEWING of any sexually explicit material;

3. Violation of any provision of Illinois School Student Records Act, which governs students' rights to privacy and the confidential maintenance of certain information including, but not limited to, a student's grades and test scores;

4. Use of PROFANITY, OBSCENITY or language that is generally considered OFFENSIVE or THREATENING to persons of a particular race, gender, religion, sexual orientation, or to persons with disabilities;

5. REPOSTING or forwarding personal communications without the author's prior consent;

6. REPOSTING or forwarding of junk mail, chain letters, or inappropriate or offensive jokes;

7. COPYING commercial software in violation of STATE, FEDERAL, OR INTERNATIONAL COPYRIGHT laws;

8. DOWNLOADING of copyrighted materials without prior authorization of the copyright holder, including but not limited to text, images, or music files;

9. DESTRUCTION, ALTERATION, or DISFIGUREMENT of hardware, software, or firmware;

10. Using the CPS Network for FINANCIAL gain or for the transaction of any BUSINESS or commercial activities;

11. PLAGIARIZING (claiming another person's writings as your own) any information gained on or through the CPS Network or any other network access provider;

12. Using the CPS Network or equipment for POLITICAL lobbying;

13. Intentionally DISRUPTING the use of the CPS Network for other users, including, but not limited to, disruptive use of any process, program, or tool for ascertaining passwords or engaging in HACKING of any kind, including, but not limited to, the illegal or unlawful entry into an electronic system, or spreading of computer VIRUSES;

14. Providing UNAUTHORIZED ACCESS to the CPS Network to unauthorized individuals, including students whose access privileges have been suspended or revoked;

15. Use of the CPS Network to violate any provision of the Chicago Public Schools Student Code of Conduct; and

16. Use of the CPS Network or equipment for soliciting or distributing information with the intent to incite violence, cause personal harm, damage a person's character, or to harass another individual.

INTERNET SAFETY

1. Student Users should never give out identifying information such as home address, school name, or telephone number in a public message such as chat room or newsgroups.

2. Student Users should avoid posting photographs of themselves in newsgroups or on web sites that are available to the public.

3. Student Users should never arrange a face-to-face meeting with someone they "meet" on the Internet without parental/guardian permission. If a meeting is arranged, the meeting should be in a public place and the student's parent/guardian should attend.

4. Student Users should never respond to messages that are suggestive, obscene, belligerent, threatening, or make a student user feel uncomfortable.

5. CPS recommends that parents/guardians read and follow the U.S Department of Justice Guidelines for Parents/Guardians on Internet Safety located at http://www.fbi.gov/publications/pguide/pguidee.htm .

ADDENDUM A Title: STUDENT ACCEPTABLE USE OF THE CPS NETWORK Section: 604.2 Board Report: 03-0326-PO03 Date Adopted: March 26, 2003 Policy:

I. **PURPOSE** This policy, also referred to as the "Student Acceptable Use for Electronic Network Related Technologies and Access Policy" ("AUP") sets forth the standards governing Chicago Public Schools ("CPS") students' use of the CPS Electronic Network Related Technologies and Access ("CPS Network") system. This policy also sets forth the rules under which student authorized users may continue their access to and use of these resources. This policy promotes the ethical, legal, and school-related use of the CPS Network and

ensures CPS compliance with the Children's Internet Protection Act. Personal electronic devices will be governed under this policy when such devices are attached to the CPS network. Authorized student use of information resources must be consistent with the educational purposes for which these resources have been provided. Use of the CPS Network is a privilege that is provided to help student authorized users complete and deliver educational obligations. The CPS Network provides student authorized users with the means for communicating effectively with schools, teachers, administrators, the public, other government entities, and educational experts. These resources should be used in a manner that both enhances students' educational experiences and complies with this policy and regulations established from time to time by the Chicago Board of Education ("Board"). CPS students, through their use of the CPS Network, will gain skills and expertise that prepare them for an increasingly technology-oriented society.

II. **DEFINITIONS** A. Chicago Public Schools' Electronic Network Related Technologies and Access ("CPS Network") is the system of computers, terminals, servers, databases, routers, hubs, switches and distance learning equipment connected to the CPS Network. These components may function in conjunction with established hardwire or wireless LAN running over outside lines, such as T-1, BRI, PRI, VPN, Dialup, Distance Learning Equipment, owned or leased by CPS. B. Distance Learning Equipment is a means for providing meetings, educational or professional courseware and workshops utilizing video and/or audio conferencing equipment, and/or media management systems to distribute video to individual classrooms and offices in schools. C. Electronic Mail (e-mail) consists of all electronically transmitted information including any combinations of text, graphics, audio, pictorial, or other information created on or received by a computer application system and includes the transmission data, message text, and all attachments. D. Internet is a worldwide telecommunications system that provides connectivity for thousands of other smaller networks. E. Other Electronic Devices include, but are not limited to, cellular telecommunication devices such as cellular phones, pagers, text communication pagers, two-way text pagers, and personal digital assistants that may or may not be physically connected to the network infrastructure. F. Password is a secret word or series of letters and numbers that must be used to gain access to an online service or the Internet or to modify certain software (such as parental controls). G. Student Authorized Users are any students enrolled in any classes offered by CPS in a traditional classroom or virtual classroom setting. H. Website is a collection of "pages" or files on the Internet that are linked together and managed by a company, institution or individual.

III. **GENERAL PROVISIONS** A. STUDENT AUTHORIZED USERS All student authorized users shall adhere to the provisions of this policy as a condition for continued use of the CPS Network. It is a general policy of CPS to promote the use of computers in a manner that is responsible, legal and appropriate. This policy is enacted anytime there is a connection to the Board's hardwired or

wireless network via outside lines such as T-1, BRI, PRI, VPN, Dialup, DSL, Distance Learning Equipment, Personal Digital Assistants, and other personal electronic devices. B. DISCLAIMER Pursuant to the Children's Internet Protection Act, CPS uses filtering software to screen Internet sites for offensive material. The Internet is a collection of thousands of worldwide networks and organizations that contain millions of pages of information. Users are cautioned that many of these pages contain offensive, sexually explicit, and inappropriate material, including, but not limited to the following categories: Adult Content; Nudity; Sex; Gambling; Violence; Weapons; Hacking; Personals/Dating; Lingerie/Swimsuit; Racism/Hate; Tasteless; and Illegal/Questionable. In general it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Student authorized users accessing the Internet do so at their own risk. No filtering software is one hundred percent effective and it is possible that the software could fail. In the event that the filtering software is unsuccessful and children and staff gain access to inappropriate and/or harmful material, the Board will not be liable. To minimize these risks, student use of the CPS Network is governed by this policy.

IV.   **TERMS AND CONDITIONS FOR STUDENT USE OF THE CPS NETWORK** A. ACCEPTABLE USES CPS students may use the various resources provided by the CPS Network to pursue educationally-related activities. Teachers and other staff should help guide students in their use of the CPS Network so that students will learn how Internet resources such as discussion boards, instant messaging and chat rooms can provide valuable educational information from classrooms, schools, and other national and international sources. In addition to using the CPS Network strictly for educational pursuits, students will be expected to follow generally accepted rules of network etiquette. These include, but are not limited to, the following: 1. Be polite. Do not become abusive in your messages to others. 2. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language. 3. Keep personal information, including the logins, passwords, addresses, and telephone numbers of students or colleagues confidential. 4. Use these resources so as not to disrupt service to other student authorized users. 5. Do not upload post, e-mail, transmit, or otherwise make available any content that is unlawful, dangerous or may cause a security risk. B. UNACCEPTABLE USES Improper use of the CPS Network is prohibited. Actions that constitute unacceptable uses of the CPS Network and are not specifically addressed elsewhere in this policy include, but are not limited to: 1. Use of the CPS Network for, or in support of, any illegal purposes. 2. Use of the CPS Network for, or in support of, any obscene or pornographic purposes including, but not limited to, the retrieving or viewing of any sexually explicit material. If a student authorized user inadvertently accesses such information, he or she should immediately disclose the inadvertent access to a teacher or to the

school principal. This will protect the user against allegations of intentionally violating this policy. 3. Use of the CPS Network for soliciting or distributing information with the intent to incite violence, cause personal harm or bodily injury, or to harass or "stalk" another individual. 4. Non-educational uses of the CPS Network including, but not limited to games, wagering, gambling, junk mail, chain letters, jokes, private business activities, raffles, fundraisers, religious activities or political lobbying. 5. Making a statement of policy, either expressly or by implication, except for messages that quote policies, Board Rules, procedures, documents published by CPS, or other official sources. 6. Using Internet tools such as discussion boards, chat rooms, and instant messaging for personal rather than educational purposes. 7. Using profanity, obscenity or language that is generally considered offensive or threatening to persons of a particular race, gender, religion, sexual orientation, or to persons with disabilities. 8. Plagiarizing any information gained on or through use of the CPS Network or any other network access provider. 9. Using copyrighted materials, including commercial software, without permission of the copyright holder, and in violation of state, federal or international copyright laws. (If students are unsure whether or not they are using materials in violation of copyright provisions, they should ask their teachers or a school technology coordinator for assistance. School based personnel are encouraged to contact the Office of Technology Services if they have questions regarding use of copyright materials found through the CPS Network.) 10. Violating of any provision of the Illinois School Student Records Act (105 ILCS 10/1et seq.), which governs students' rights to privacy and the confidential maintenance of certain information including, but not limited to, a student's grades and test scores is prohibited. 11. Using the CPS Network for financial gain or for the transaction of any business or commercial activities. C. SECURITY All student authorized users are to report promptly any breaches of security violations of acceptable use and the transmission of web addresses or e-mail information containing inappropriate material (as outlined in Section III B of this policy) to their teacher or the school principal. Authorized personnel will report such breaches to the Area Instructional Officer or designee or the Chief Technology Officer or designee of the Chicago Public Schools. Failure to report any incident promptly may subject the student authorized user to corrective action consistent with the Uniform Discipline Code ("UDC"), Board's rules, and policies. In order to maintain the security of the CPS System, students are prohibited from engaging in the following actions: 1. Connecting to a modem to dial into any online service provider, or Internet Service Provider ("ISP") or connect through a Digital Subscriber Line ("DSL") while physically being connected to the CPS Network where a T-1 line is functioning. 2. Intentionally disrupting the use of the CPS Network for other users, including, but not limited to, disruptive use of any processes or programs, sharing logins and passwords or utilizing tools for ascertaining passwords, or engaging in "hacking" of any kind, which is an illegal or unlawful entry into an electronic system to gain secret unauthorized information. 3. Intentionally spreading

computer viruses or programs that loop repeatedly, or for the purpose of infiltrating a computer system without authorization or for damaging or altering without authorization the software components of a computer or computer system. 4. Disclosing the contents or existence of CPS computer files, confidential documents, e-mail correspondence, or other information to anyone other than authorized recipients. Student authorized users must not share logins or password(s) and unauthorized information regarding other users' passwords or security systems. 5. Downloading unauthorized games, programs, files, electronic media, and/or stand-alone applications from the Internet that may cause a threat to the CPS Network.

V. **STUDENT WEBSITES** 1. Educational Purposes Student authorized users may create webpages as a part of a class activity. Material presented on a student's class activity website must meet the educational objectives of the class activity. CPS has the right to exercise control over the content and/or style of the student webpages. Only those students whose parent(s) or guardian(s) have completed the attached Consent Form and Release (Attachment A) may post their work or picture on student or school websites. Students whose work, likeness (as captured by photograph, video or other media) or voices are presented on a student website shall be identified by first name only for confidentiality and safety purposes. 2. Website Development Students designing websites should go to www.schoolhosting.cps.k12.il.us for the directions and procedures they need to follow in developing their websites. VI. MONITORING The CPS Network is routinely monitored to maintain the efficiency of the system. Student authorized users should be aware that use of the CPS Network, including their use of e-mail, is subject to reasonable and appropriate monitoring by OTS/MLA that abides by the requirements of all applicable state and federal laws. Any activities related to or in support of violations of this policy and/or the UDC may be reported and will subject the user to sanctions specified either in the UDC or in this policy.

VI. **ASSUMPTION OF RISK** CPS will make a good faith effort to keep the CPS Network system and its available information accurate. However, student authorized users acknowledge that there is no warranty of any kind, either express or implied, regarding the accuracy, quality, or validity of any of the data or information available. For example, and without limitation, CPS does not warrant that the CPS Network will be error free or free of computer viruses. In making use of these resources, student authorized users agree to release the Board from all claims of any kind, including claims for direct or indirect, incidental, or consequential damages of any nature, arising from any use or inability to use the network, and from any claim for negligence in connection with the operation of the CPS Network. Student authorized users further acknowledge that the information available through interconnecting networks may be inaccurate. CPS has no ability to maintain such information and has no authority over these materials. CPS makes no warranty of any kind, either express or implied, regarding the accuracy, quality, or validity of the data and/or information residing on or passing through the CPS Network from outside networks. Use of the CPS Network is at the risk of the student authorized user.

VII. **INDEMNIFICATION** The student authorized user indemnifies and holds the Board harmless from any claims, including attorney's fees, resulting from the user's activities while utilizing the CPS Network that cause direct or indirect damage to the user, CPS, or third parties.

VIII. **SANCTIONS** Failure to abide by this policy may subject the student authorized user to corrective action ranging from suspension of some or all access privileges up to and including expulsion and prosecutions according to the UDC. A violator must understand that if his or her privileges to use the CPS Network are revoked by a school faculty member that he or she has the right to appeal the revocation within thirty (30) days, in writing, to the principal of the school. The school principal's decision shall be FINAL. If an student authorized user's access to the CPS Network is suspended by CPS Network administrators as a result of violations of this policy, the student may appeal the suspension to the Chief Education Officer or designee. A violator must understand that if he or she is removed from the CPS Network, there shall be no obligation to provide a subsequent opportunity to access the CPS Network. Amends/Rescinds: Rescinds 02-0626-PO04 and 97-0325-PO2 Cross References: Legal References: 105 ILCS 10/1 et seq. (Illinois Student Records Act); Pub. L. No. 106-554 (Children's Internet Protection Act).

ADDENDUM B

MLA 1:1 Chromebook Program Liability Document

Computers obtained through the MLA come with a three-year warranty, which covers any hardware-related problems due to manufacturer's defect. The MLA Technology Department will coordinate ALL hardware repairs with the manufacturer. The Technology Help Desk will be open before, during, and after school, on school days. Students will be given a replacement computer.

Student and Parent(s)/Guardian(s) shall bear the risk of loss for a lost, stolen, or damaged computer or accessories due to accident, neglect or negligence from the date the student receives the computer until the return of the computer to MLA, and shall be liable to MLA for the replacement cost and other damages caused by such loss, theft, or damage due to accident, neglect or negligence as set forth in the Marine Leadership Academy Student Chromebook Program Consent Form not covered by manufacturer's warranty as specified and further described in the MLA Liability Document. MLA strongly recommends parents personally insure the computer on their own personal homeowners or renters policy as a rider, if necessary, to cover these costs. Repair of a computer that is accidentally damaged - dropped, spilled on, zapped by an electrical surge, etc. (what is referred to as "end user damage") - will not be covered by the manufacturer's warranty and is the responsibility of the Student and Parent(s)/Guardian(s).

The current costs to replace miscellaneous parts that are damaged by the user, lost or stolen:

- AC Power Adapter: $50
- Screen $40
- Chromebook: $300

If a repair is software related, the computer will be restored to its original software configuration free of charge.

Hardware upgrades or modifications to the computer are not allowed. Should modifications be made to the computer, such modifications will become the property of MLA. MLA has the right to restore the computer to its original state whenever we feel it is appropriate and necessary. Anything that is loaded on the local drive will be deleted. Students are responsible for backing up their school related files to an external drive or the cloud on a regular basis.

MLA Student Chromebook Program Frequently Asked Questions (FAQ):

Technology in the Classroom

Why 1:1 Computing? The purpose of the MLA Student Chromebook Program is to prepare students for their future, a global digital world where they will be expected to use information and technology to create, examine, explore, communicate and collaborate. Students leverage mobile computing at school and at home for their coursework, research, and collaboration. Integration of technology in the classroom expands the possibilities of teaching and learning.

How will this help my child as a student? Integrating technology into the classroom will extend the learning experience beyond the confines of the classroom by leveraging technology to solve problems, gather and evaluate information, and disseminate work efficiently. Technology allows for immediate feedback to both students and instructor about student understanding during direct instruction and classwork, enabling the instructor to optimize learning experiences for students in real time. One-to-one computing facilitates student focus and attentiveness in class through learning that is either self-paced and individualized or collaborative and cooperative.

How will they be using technology in class? In class and at home, students are provided with digital spaces for collaboration. This allows for seamless transitions from classwork to homework, whether class collaborators live across the street or across town. We find this is a huge benefit, as students can't always meet easily to work on projects or have other commitments with sports, clubs, jobs, etc.

In Algebra, teachers provide audio/visual lectures. In flipped classroom lectures, students have the ability to replay portions of lectures in order to better understand complex processes. In Physics, students have access to interactive modeling software that enables them to understand abstract concepts in mechanics, replaying interactions with different variables to arrive at a deeper understanding of concepts. In English and Social Science,

students are given texts in a manner that is more interactive than mindless copying of prepared notes.

Finally, as high-stakes assessments (ACT, SAT, GRE, etc.) are increasingly being administered online, the skill of navigating computer-based assessments is becoming increasingly valuable. Strategies and methods are markedly different. The more experience students have with computer-based assessments, the more accurately the assessment will measure their knowledge, as opposed to measuring their lack of familiarity with the test format.

Will this eliminate the personal touch of teaching? Not at all! Our goal is to have the students equipped with a tool that increases engagement and achievement, and individualizes student's learning experiences. Teachers recognize that technology integration is only one of the many tools they can and should utilize in the design and implementation of lessons. The relationship between teacher and student is an important one and will not be replaced by the use of computers in the classroom.

Will having computers make the students isolated? Studies show that students involved in one-to-one computing programs increase communication with teachers and other students. They also increase their teamwork skills. The computers also lend themselves to enhancing projects done as a group.

Will computers in the classroom be distracting? Computers are a tool that must be managed, just like pen and paper. The teacher is in control of the class and at any time can tell students to close the screens in order to have their full attention.

Will this enable cheating or plagiarism? All computers will have software installed that allows teacher monitoring of the computers during class time. This monitoring is a huge deterrent to misuse. Also, many classes already require students to submit any written work to Turnitin.com, an on-line plagiarism service to which MLA subscribes. Cheating and plagiarism are always considered very serious offenses and are dealt with according to the CPS Student Code of Conduct. MLA will continue to help students understand and apply responsible and ethical standards in their work.

Financial

Is there a cost participate in the program? No. The school owns the computer. Students participating in this program will be given a computer that they will use in their classes for instruction. Beyond mere note-taking, the use of the computer is incorporated into all aspects of the class: classwork, homework, & assessment. Students develop 21st century skills, collaborating with students around the corner and around the world.

Why would I want my child to spend more time on the computer? In the past, intensive users of technology were stereotyped as loners. Today, we understand that digital spaces are social spaces; thus, intensive users of technology are extremely social today. In the future, students will interact socially and professionally in was that are difficult to imagine. In this program, students have the opportunity to practice digital social skills within the context of

supervised regular school work. Habits acquired in this environment are translatable to future social and professional situations.

What do you mean when you say 21st century skills? One example is the issue of information layering. In a paper world, we tend to think in a linear way, a succession of pages of static text. Digitally, information is increasingly being layered. Becoming skilled in the layering of information in digital texts is increasingly becoming a crucial academic and professional competency.

Since my child uses technology all of the time, doesn't she already have these skills? All around us, we see many people passively using technology to move pictures around, watch videos, and send snippets of text. In response to a growing number of people using technology to passively consume, the definition of digital literacy is evolving. Today, digital literacy describes technology users who are able to produce, rather than just consume; to be digitally literate means more than simply using a computer, it means using technology to solve problems.

I just bought a computer. Why can't my child just use that? Chicago Public Schools only allows personal computers on our guest wireless network. For security reasons computers on the CPS guest wireless system cannot access any resource behind the CPS firewall. Personal computers will not have access to the school website, school e-mail, network files or additional class management systems.

What if there is a problem with this computer? Students receive on-site, real time tech support at MLA. If the technology department can't immediately fix the students computer we will give them a spare replacement computer. Furthermore, the fact that the technology support is school- based, your son or daughter assumes the responsibility of resolving issues, becoming more self assured and independent in the process. There is no other warranty program that provides the scope of these services.

What is included? A Chromebook computer, AC adapter/power supply, manufacture warranty and on-site tech support.

Why is this better than buying whatever computer I want from another retailer? If you purchase your own computer, you may not connect to the CPS network at school. Unfortunately, you are only allowed to connect to the school's guest wireless network per Chicago Public Schools security policy. The guest wireless network does not have access to CPS mail, files or our class management software which are all needed for instruction, even in non-1:1 classes. Additionally, no other warranty will provide on-site service and a spare computer while yours is being fixed. No calling an 800 number for support. Your son or daughter simply comes to the Technology Department Office when they have time.

What happens if the computer does not work or is accidentally damaged? Computers obtained through MLA come with a manufacture warranty which covers any hardware-related problems due to manufacturer's defect. The MLA Technology Department will coordinate hardware repairs with the manufacturer. While the machine is being repaired, the student will be given a replacement computer. The Technology Help Desk will be open before, during, and after school, on school days.

Student and Parent(s) shall bear the risk of loss for a lost, stolen, or damaged computer or accessories due to accident, neglect or negligence from the date the student receives the computer until the return of the computer to MLA, and shall be liable to MLA for the replacement cost and other damages caused by such loss, theft, or damage due to accident, neglect or negligence as set forth in the Marine Leadership Academy Student Chromebook Program Consent Form not covered by manufacturer's warranty as specified and further described in the MLA Liability Document. MLA strongly recommends parents personally insure the computer on their own personal homeowners or renters policy as a rider, if necessary, to cover these costs.

Repair of a computer that is accidentally damaged - dropped, spilled on, zapped by an electrical surge, etc. (what is referred to as "end user damage") - will not be covered by the manufacturer's warranty. The costs to replace miscellaneous parts that are damaged by the user, lost or stolen:

- AC Power Adapter: $50
- Screen $40
- Chromebook: $300

If a repair is software related, the computer will be restored to its original software configuration free of charge.

Hardware upgrades or modifications to the computer are not allowed. Should modifications be made to the computer, such modifications will become the property of MLA.

MLA has the right to restore the computer to its original state whenever we feel it is appropriate and necessary. Anything that is loaded on the local drive will be deleted. Students are responsible for backing up their files to a USB flash drive or external hard drive provided by the student.

Just to make sure, if there is a problem that is due to manufacture defect do I have to pay? All repair of defective hardware is covered under the manufacturer warranty and is of no cost to you.

If I drop the unit and crack the screen or spill water on it, do I have to pay? All end-user damage and accidental damage is 100% the responsibility of the family.

What if the computer is stolen or destroyed? Warranty does not cover theft or total destruction of the computer due to accident or neglect. Parents are advised to add the computer, as a rider if necessary, on their own homeowner's/renter's insurance policy to cover this. The student is responsible for the computer while it is in his/her possession. If your computer is lost or stolen, please bring it to the attention of the Technology Department immediately by e-mailing skhaderlein@cps.edu or eesoto@cps.edu with the student name, parent name, parent contact information, insurance company contact

information and in the case of theft, a copy of the police report or police record number. Who will own the computer? MLA owns the computer.

Responsibilities

What are my responsibilities? Participation in the MLA Student Chromebook Program is a privilege that fosters great power. With great power comes great responsibility. Students and their families are responsible for keeping the computer safe and in working order and your CPS network credentials secure. DO NOT share your CPS network username and password with others. Parents must remember while the primary function of the computer is school work and students may be expected to complete homework on the computer in your home, YOUR rules apply to this computer. You the parent are responsible for setting expectations and limitations for use at home. Families should discuss appropriate and inappropriate websites, online safety and how to best monitor student use at home. We will discuss these topics more in our on-line training modules.

What are acceptable uses of this and all MLA/CPS technology? The Chicago Public Schools ("CPS") Student Acceptable Use of the CPS Network Policy (AUP) sets forth the standards governing CPS students' use of the CPS Electronic Network Related Technologies and Access ("CPS Network") system. This policy also sets forth the rules under which student authorized users may continue their access to and use of these resources. This policy promotes the ethical, legal, and school-related use of the CPS Network and ensures CPS compliance with the Children's Internet Protection Act. The CPS AUP is attached or available at http://policy.cps.k12.il.us/documents/604.2.pdf, must be read and will be agreed to by signing the attached Consent Form. What happens if the student breaks the guidelines of the AUP? Failure to abide by this policy may subject the student to corrective action according to the CPS Student Code of Conduct as deemed appropriate by the Technology Director and the Dean of Students.

What do I do if the computer is lost or stolen? If your computer is stolen, complete a police report with your local police department. In the case of either loss or theft, contact your insurance company to file a claim. Then bring the loss to the attention of the Technology Coordinator by e-mailing skhaderlein@cps.edu or eesoto@cps.edu with the student name, parent name, parent contact information, insurance company contact information and in the case of theft, a copy of the police report or police record number.

Logistics

Will this make the back packs heavier? MLA will be introducing e-texts, digital resources and on-line curriculum throughout the upcoming years. Some classes will also use a physical textbook with the computer. Use of the computer as a notebook will help to eliminate many of the binders, papers, books, and colored pens the students now carry in their backpacks.

Will I need an internet connection? Yes. Internet access is available at MLA and at all Chicago Public Libraries (see http://www.chipublib.org/aboutcpl/wifi.php for more information). If your child is eligible to participate in the National School Lunch Program, you may qualify for Comcast's Internet Essentials Program. Visit

http://www.internetessentials.com for more information. Will textbooks be available online? We will be introducing e-text, digital resources and on-line curriculum throughout the year. Some classes will also use the physical textbook with the computer.

Will the computers be used in each class every day? We do not promote the use of technology for technology's sake. The computer provides spontaneous, active learning through Internet research, data collection and analysis, and collaboration. Use of the computer in class will depend on the content area and the appropriateness of technology for the lesson being taught. It is expected that the type and frequency of use will vary according to the curriculum. Students will also take advantage of the anywhere-anytime learning possibilities of the computer as well as using it outside of the classroom environment.

Can my child bring the computer home at night and on weekends? Yes. The computer is for the student's use at school and home. All data and personal software is the responsibility of the student.

How will the computer connect to the school's wireless network? The computer has a built-in wireless networking card that will connect to MLA' school-wide secure wireless network.

How will the computer connect to home networks? Computers will connect to standard 802.11b, g or n wireless networks at home. Please refer to your home internet service provider for more information.

What about battery life? The computer has a primary battery that has an expected life of 6-8 hours. Students are required to plug in their computers each night so that they will have fully charged batteries for the next school day.

What about printing? The computer will be able to print to multiple networked printers at school located on every floor of the school. School network printers are monitored and regulated through print management software. The computer has two USB ports and built-in wireless to connect to printers and networks at home. As the trend toward digital documents is realized more and more in the classroom, most documents are communicated digitally between students and teachers, thus eliminating the need for printing.

Support

Can you help me setup my home printer, wireless, network connection, etc.? No. We cannot be responsible for support for any devices or networks outside of the school. You may want to call a local fee for service Tech Support Company such as Geek Squad for assistance with home tech services.

What happens to my child's files if something happens to the computer or hard drive, for example? Students are responsible for their data. Students have 5GB of space available via CPS' Google Apps for Education account and should save their files to this space on the cloud so it is accessible from any computer or device that can connect to the internet.

What are the computer specifications?

- System Type: Samsung Chromebook 11
- Processor: 5 /1.7 GHz, Samsung Exynos 5
- Operating System Google Chrome OS
- System Memory: 2 GB
- Hard Drive: 16 GB
- Display: 11.6 in LED Backlit
- Communications: Integrated 10/100 LAN, .3 Mega Pixel Webcam
- Integrated Wireless: WLAN (B/G/N), Bluetooth
- Battery: 2-cell Lithium polymer
- Power: 65W AC Adapter / Charger
- For any other questions please contact Steve Haderlein, at skhaderlein@cps.edu.
  or Esmeralda Soto at eesoto@cps.edu