

---

# **Acceptable Use Policy**

**for**

# **Technology**

**Version 2.0**

# **Metro Early College**

# **High School**

**August 2012**

## Table of Contents

Table of Contents .....2

1. Note .....3

2. Acceptable Use .....3

3. Availability of Access .....4

4. Monitored Use .....6

5. Disclaimer of Liability .....6

6. Training .....6

7. Copyright.....6

8. Network Access.....6

9. Network Coordinator.....7

10. *Individual User Responsibilities*.....7

    10.1 Acceptable Use.....7

    10.2 Standards of Acceptable Use .....7

        10.2.1 Standard One .....8

        10.2.2 Standard Two.....8

        10.2.3 Standard Three.....9

        10.2.4 Standard Four .....9

        10.2.5 Standard Five.....9

        10.2.6 Standard Six.....9

        10.2.7 Standard Seven .....10

        10.2.8 Standard Eight .....10

        10.2.9 Standard Nine .....10

        10.2.10 Standard Ten (Personal Safety) .....10

11. Vandalism Prohibited .....10

12. Forgery Prohibited.....11

13. Limitation, Termination and/or Revocation of Privileges.....11

14. Warning .....11

15. Safety Issues .....11

16. Internet Access .....11

    16.1 Terms and Conditions of Use.....12

    16.2 Procedures for Use .....12

    16.3 Rules Governing Use .....13

    16.4 Penalties for Improper Use.....15

    16.5 Warranty.....15

    16.6 Security .....15

    16.7 User Privacy .....15

    16.8 School Policies .....15

17. Other .....16

18. Code of Conduct – Your copy .....17

19. Signature – Code of Conduct .....18

## Revision History

Name	Date	Reason For Changes	Version
Education Council	03/31/08	Conception	1.0
Metro High School	8/1/2012	Updates	2.0

## Note

Metro Early College High School (the “School”) computers, personally-owned devices that access the School’s Network, and the use of the School Network, Internet access, the electronic communications system and/or on-line services (collectively, the “Network”) support learning and enhance instruction, as well as assist in administration. All students and staff members must have a signed AUP form on file before they have access to technology and Internet services.

### USE OF TECHNOLOGY RESOURCES

Purpose: To establish School’s vision and the basic structure for the use of technology resources.

## 1. Acceptable Use

The School’s Chief Academic Officer or his/her designee will implement, monitor and evaluate electronic media resources for School purposes.

The purpose of the School’s Network is to support research and education in and among institutions by providing access to unique resources and the opportunity for collaborative work. All use of the Internet and Network must be in support of education and research and be consistent with the educational objectives of the School. Use of other networks or computing resources must comply with the rules governing those networks. Transmission of any material in violation of any federal or state laws or regulations and FERPA rules are prohibited; this includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secret. Access to computer Networks and Networks owned or operated by the School is subject to internal policies and local, state, and federal laws.

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, Network security mechanisms, and the individual’s rights to privacy and freedom from intimidation, harassment, discrimination, and unwarranted annoyance.

The School will have the following in continuous operation, with respect to any computers belonging to the School and having access to the Internet:

1. A qualifying technology protection measure, as required by CIPA. The protection measures are designed to block or filter internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors; and
2. Procedures or guidelines that provides for monitoring the online activities of users and the use of the chosen technology protection measure to protect against access through such computers to visual depictions that are obscene, pornographic, or harmful to minors, as those terms are defined in CIPA.

Such procedures or guidelines will be designed to:

1. Provide for monitoring the online activities of users to prevent, to the extent practicable, access by minors to inappropriate matter on the Internet and the World Wide Web;
2. Promote the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

3. Prevent unauthorized access, including so-called "hacking," and other unauthorized activities by minors online;
4. Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors; and
5. Restrict minors' access to materials "harmful to minors," as that term is defined in CIPA.

Pursuant to Federal law, students shall receive education about appropriate on-line behavior, including: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors while interacting with other individuals on social Networking websites, using e-mail, chat rooms, other forms of direct electronic communications, and cyberbullying awareness and response; (c) unauthorized access (e.g., "hacking") and other unlawful activities by minors on line; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) measures restricting minors' access to materials harmful to them.

## **2. Availability of Access**

The School will make access to the School's Network, including the Internet, available to students and employees exclusively for instructional and administrative purposes and in accordance with administrative rules.

Access to the School's Network is a privilege, not a right. All users will be required to acknowledge receipt and understanding of all administrative rules governing use of the Network and will agree in writing to comply with rules and guidelines. Noncompliance with applicable administrative rules will result in disciplinary action consistent with School policies and administrative rules up to and including termination of employment or expulsion of students. Violations of law may result in criminal prosecutions, as well as disciplinary action by the School and or its affiliates.

In order to enhance the learning experience, students may bring personally-owned computers or other web-enabled devices to school for use in curricular and extra-curricular activities ("Bring Your Own Devices" or "BYOD") as approved by a teacher, coach and/or administrator (a "School Official"). Pursuant to BYOD, students will be allowed to access the Network for approved activities, projects and/or assignments. Because the Network is meant to support your educational progress, you are not allowed to access it for personal uses.

The School reserves the right to approve the types of devices that it will allow to access the Network. The approval is subject to change at the School's sole discretion at any time. All approved devices must allow access to the Internet through a fully functional web browser and be capable of accessing the MHS Network. All Internet access shall occur using the MHS Network. Cellular Network adapters are not permitted to be used by students to access the Internet at any time.

The use of personal technology to provide educational material is not a necessity but a privilege. A student does not have the right to use his or her laptop, cell phone or other electronic device while at school. When abused, privileges will be taken away. When respected, privileges will benefit the learning environment. The School will establish rules governing when and where Technology may be used.

The School accepts no responsibility for personal property brought to the school. Personally-owned laptops or other devices that are stolen or damaged are the responsibility of the student and their parents/guardians. The School's information technology personnel are not responsible for repairing and/or maintaining privately-owned devices. The owner of the device is solely responsible for ensuring that the device is in good working order.

Students and parents/guardians participating in BYOD must adhere to all School policies and the Acceptable Use Policy. Additionally:

1. The device will not be used in the hallways, bathrooms or parking lots unless otherwise directed by a School Official. Students are prohibited from using head phones or ear buds in the hallways, bathrooms or parking lots unless otherwise directed by a School Official.
2. The device must be in silent mode while on school campuses unless otherwise directed by a School Official.
3. The device may not be used to cheat or assist cheating on assignments or tests or for non-instructional purposes during instructional time.
4. The device may not be used to record, transmit or post photographic images or video of a person, or persons on campus during school activities and/or hours unless assigned by a School Official as allowed by the Acceptable Use Policy.
5. The device may only be used to access files or internet sites which are relevant to the classroom curriculum. Non-instructional games are not permitted.
6. Students must comply with a School Official's request to turn off the device.

Students acknowledge and agree that:

1. The School's Network filters will be applied to all access to the internet and should not be circumvented. Any attempt to circumvent the filters is a violation of the Acceptable Use Policy and will subject the user to loss of privileges, discipline and/or referral to law enforcement.
2. The School may take possession of and examine any device when School personnel observe or reasonably suspect that a device is being used in violation of these rules or that a search is required to discover evidence of a violation of law or other School rules, including but not limited to the Acceptable Use Policy.
3. Personal technology must be charged prior to bringing it to school and the device must run off its own battery while at school.
4. The students remain subject to all other School behavior rules and the Code of Conduct. Violation of the BYOD provisions of this policy may lead to discipline under the Code of Conduct and/or confiscation of the device. The device may be confiscated even if the student does not own the device. Confiscated devices will be released to the parent of the student upon request. Confiscated devices will be released to the student when the disciplinary consequences have been served or at the end of the school year, whichever is sooner.

### **3. Monitored Use**

Students and employees should have no expectation of privacy in their use of the Network and/or their use of the Network to transmit or receive electronic mail or other messages. Designated staff may monitor these actions at any time to ensure appropriate use for educational or administrative purposes, for maintenance or repair, or for no reason.

### **4. Disclaimer of Liability**

Users accept all risks attendant upon the use of the Network, without exception. The School will not be liable for loss, damage, inconvenience, or any other harm or damages resulting from the use of the School's Network, including but not limited to user misuse including violations of copyright restrictions, users' mistakes or negligence or costs and /or charges for service incurred by users. The School is not responsible for ensuring the accuracy or usability of any information found on the Internet, or for the suitability of the Network for any particular use.

The Chief Academic Officer or his/her designee will oversee the School's Network and is the final authority over any and all aspects of its use.

Oversight of the posting of official School, campus or division/department materials on the Network will be the responsibility of the Chief Academic Officer, principal or division/department supervisor or his/her designee.

The Network will be used only for administrative and instructional purposes consistent with the School's mission and goals.

### **5. Training**

It is the goal of the School to provide training for employees and students, and management or teachers will answer any user questions regarding the proper use of the Network and provide copies of the School's acceptable use guidelines for users. Teachers and managers will emphasize ethical use of the Network's resources.

### **6. Copyright**

Users shall abide by copyright law, and shall respect the intellectual property rights of authors and creators without exception. Violation of copyright may lead to disciplinary action up to and including termination or the expulsion of students. Copyrighted software or data may not be placed on any Network connected to the Network without documented permission from the holder of the copyright. Only the owner or individuals the owner specifically authorizes may upload copyrighted material to the Network.

### **7. Network Access**

Access to the Network will be governed as follows:

- With the approval of the principal or division/departmental supervisor or his/her designee, users will be granted appropriate access to the Network subject to this policy and all applicable policies, regulations and law.
- Any Network users identified as having violated School, campus and/or division/department Network acceptable use guidelines, policies, or law will be subject to disciplinary action consistent with School policies and administrative rules up to and including termination of employment or expulsion of students.

## **8. Network Coordinator**

The Network coordinator (center coordinator or his/her designee) for the electronic communication Network will do the following:

- Disseminate and enforce applicable School as well as University policies and acceptable use policies for the School's Network
- Ensure that all users of the School's Network complete and sign an agreement to abide by School policies and administrative rules regarding such use. All such agreements will be kept on file by the human resource coordinator
- Ensure that all employees supervising students who use the School's Network provide education and training emphasizing the appropriate uses of these resources
- Monitor or examine Network activities as appropriate to ensure proper use of the Network
- Set limits for storage of data and other technical parameters for users of the Network, as needed or as directed from School level technology staff

## **9. Individual User Responsibilities**

### **9.1 Acceptable Use**

Activities in direct support of teaching and learning, such as professional development, administrative communications, grant applications, new project announcements and student product publishing, are acceptable. It is the general policy that School Network facilities are to be used in a responsible, efficient, ethical and legal manner in accordance with the instructional mission of the School, the acceptable use and other School policies, and applicable local, state and federal law(s). Faculty and students must acknowledge by signature their understanding of the general policy and guidelines and their agreement to abide by those policies as a condition of receiving access to the Network.

### **9.2 Standards of Acceptable Use**

Failure to adhere to this policy and the standards within may result in disciplinary action, including revocation of the offender's Network access privilege by the Network administrator, termination of employment and expulsion of students.

Willful misuses may lead, in addition to serious disciplinary action, to criminal prosecution under applicable state and federal law. The standards do not attempt to articulate all permitted or prohibited behavior by users and require application of common sense in light of the purpose and

general policy for Network and Internet access. The Chief Academic Officer shall have the final authority over decisions regarding acceptability of use. It is the responsibility of users to seek the approval and guidance of management or teaching staff if there is any question of the acceptability of a specific proposed use, and the responsibility of such managers or teachers to seek appropriate guidance in cases of uncertainty.

### **9.2.1 Standard One**

Acceptable uses of the Network are activities which support learning and teaching. The School encourages Network users to develop uses which meet their individual needs and which take advantage of the Network's functions, including but not limited to:

- Databases
- Internet resources
- Conferences and publishing

### **9.2.2 Standard Two**

Unacceptable uses of the Network include, but are not limited to, the following:

- Accessing the password protected materials of any student or employee, or of any third person or entity.
- Transmitting profanity, obscenity or other communications in any form or medium which may be offensive to the recipient to any individual, group, web site, news group, mailing list or similar forum
- Downloading, storing or printing files or messages (text, sound, still or moving graphics or any combination thereof) that are pornographic or obscene or that use language, sounds or imagery which offends or tends to degrade others (the designated official in the administration shall have the final authority to determine suitability in particular circumstances)
- Transmitting any material which is threatening to another person, group or the general community, whether or not such material is transmitted to that third person
- Copying proprietary information, including software, in violation of applicable law and policy
- Using the Network for personal financial gain, business activity not on behalf of the School or any illegal activity
- Knowingly or negligently transmitting or opening the Network to the reception of computer viruses and other malware or failing to scan downloaded files for viruses
- Deliberately trying to degrade or disrupt Network performance (such acts will also be viewed as criminal activity under applicable state or federal law)
- Re-posting personal communications without the author's prior consent
- Transmitting product advertisement, political lobbying, chain letters or "spamming"
- Personal use not related to educational purposes, including the playing of games
- Knowingly or maliciously falsifying or corrupting data, including changing grades, attendance data, financial data, etc. for personal gain or vandalism purposes
- Any other use deemed not consistent with the School policy or mission in the sole discretion of the Chief Academic Officer



- Purchasing items via a credit card number or other electronic payment Network or obligating another staff member, student or the school to pay
- Sending or receiving messages or information with someone else's name
- Participating in any electronic "chat" unless it is for specific educational purposes, authorized in advance and directly supervised by staff
- Accessing offsite personal e-mail accounts
- Using the Network for any purpose that wastes the time of employees and/or students, or that wastes limited Network resources including but not limited to printing supplies and bandwidth

### **9.2.3 Standard Three**

Employees may have their own e-mail accounts. Teachers will act as sponsors for students using any e-mail accounts set up for classroom use. E-mail accounts are secured for educational purposes only. No individual student account will be created for the general use of a student. The user has no expectation of privacy in any communication made using the Network or stored on the Network, and the school Network reserves the right to access and review all electronic messages transmitted on any Network provided by the school Network. Sponsors are responsible for guiding student access to appropriate sections of the Network and for assuring that students understand that misuse of the Network may cause them to lose their accounts and/or face disciplinary action. Where appropriate, sponsors will assume responsibility for teaching the students proper techniques and standards for participation and explaining issues of privacy, copyright infringement, tool use and Network etiquette.

### **9.2.4 Standard Four**

All users will abide by prevailing etiquette rules for net usage, including etiquette rules specific to a web site, news group, mailing list or other forum, and shall not violate the terms of service of any such service or forum.

### **9.2.5 Standard Five**

The Network may not be used for illegal purposes, in support of illegal activities or for any other activity prohibited by School policy or not in keeping with the School's mission or moral standards of the community.

### **9.2.6 Standard Six**

Network users may not use another person's Network or e-mail ID or password or share their own with others.

#### **Password Confidentiality**

Each individual is responsible for the confidentiality of his/her personal password or any password assigned to him/her for the purpose of fulfilling an assigned job task. The individual will be responsible for breach of security caused by the sharing of passwords. The School will cooperate fully with local, state or federal officials in any investigation concerning or relating to any misuse of a password, such as using it to enter a program for the sole purpose of gaining confidential information, changing data or placing false

information or data into the Network or doing the same over the internet. The School may limit, suspend or revoke a Network user's access to the School's Network upon violation or misuse of any password, or take disciplinary action up to and including termination of employment or expulsion of a student.

### **9.2.7 Standard Seven**

Network users will maintain electronic information in accordance with established guidelines.

### **9.2.8 Standard Eight**

Network users may not upload programs to the School's Network or download and install programs from internet sources without appropriate authorization.

### **9.2.9 Standard Nine**

Network users may not knowingly bring prohibited materials into the School's Network.

### **9.2.10 Standard Ten (Personal Safety)**

Network users will not post personal contact information about themselves or other people. Personal contact information includes personal address and telephone numbers. Network users will abide by all State and Federal laws and School policies relating to the privacy of students and their families, and will not allow such data to come into the possession of any unauthorized user.

Students will not agree to meet with someone they have met online. (Students will not communicate on-line with anyone they do not know).

Students will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable, or any solicitation by any person to meet, exchange personal information, or make contact in any form.

Users who violate these standards may be subject to disciplinary action in accordance with School policy and/or legal actions.

## **10. Vandalism Prohibited**

Any malicious attempt to harm or destroy School equipment or materials, data of another user of the School's Network or any of the agencies or other Networks that are connected to the Internet is prohibited. Deliberate attempts to compromise, degrade or disrupt Network performance may be viewed as violations of School policies and administrative rules and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses.

## **11. Forgery Prohibited**

The School prohibits forgery or attempted forgery of electronic mail messages. Attempts to read, delete, copy or modify the electronic mail of other Network users or deliberate interference with the ability of other Network users to send/receive electronic mail is prohibited. This does not, however, limit or modify in any way the School's right to monitor use.

## **12. Limitation, Termination and/or Revocation of Privileges**

The School may limit, suspend or revoke a Network user's access to the School's Network, or take disciplinary action up to and including termination of employment or expulsion of a student upon violation of any of the School policy or administrative rules regarding acceptable use.

## **13. Warning**

Network users and parents of students with access to the School's Network should be aware that use of the Network may provide access to other electronic communication Networks in the global electronic network that may contain inaccurate or objectionable material.

## **14. Safety Issues**

The School's Network is provided on an "as is, as available" basis. The School does not make any warranties whether express or implied with respect to any services provided by the Network and any information or software contained therein. The School does not warrant that the functions or services performed by, or that the information or software contained on, the Network will meet the Network user's requirements or that the Network will be uninterrupted or error-free or that defects will be corrected.

Opinions, advice, services and all other information expressed by Network users, information providers, service providers or other third party individuals in the Network are those of the providers and not the School. Users shall not imply to any person or group that their communications over the internet represent the views or position of the School unless such communication has been previously approved as official.

The School will cooperate fully with local, state or federal officials in any investigation concerning or relating to misuse of the School's Network.

## **15. Internet Access**

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

- Locally Networked reference and research sources;

- Worldwide and local electronic mail services;
- Global information and news;
- Public domain and shareware computer software of all types;
- Discussion groups on a vast range of topics; and
- Local, regional, public, state, and national library catalogs

The availability of Internet access provides a unique opportunity for students and staff to contribute to the School's presence on the World Wide Web. This medium of communication provides an opportunity to share accurate information with the community, state, and world about the School's curriculum and instruction. This resource serves as an educational tool for staff and students, and its use will be governed by the Internet Acceptable Use policy. The failure to follow these policies or responsibilities may result in the loss of privileges or other disciplinary measures.

With access to computers and people all over the world also comes the availability of materials; however, on a global Network it is impossible to control access to all materials, and the valuable information and interaction available on this worldwide Network far outweighs the possibility that users may procure material that is not consistent with the educational goals of the School.

The smooth operation of the Internet Network 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 the Internet. Any violations of these guidelines will subject the user to appropriate disciplinary action and possible denial of access to the Internet. In general, this requires efficient, ethical, and legal utilization of the Network resources.

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

Prior to accessing the Internet, students and staff will receive instruction on the appropriate use of the Internet. In addition, parents will be required annually to sign a permission form before students will be allowed access.

## **15.1 Terms and Conditions of Use**

### **15.2 Procedures for Use**

Staff may access the Internet for educational or work-related purposes at any time and in a manner which is not disruptive and does not interfere with the performance of other responsibilities by the employee or other staff members.

Students will be allowed to access the equipment and obtain Internet access only through their teachers and provided they have returned the signed permission form for use. No students may access the Internet without permission, and such access is NOT for the student's general use but for specific activities related to their education. Student use must be supervised at all times by a staff member.

### **15.3 Rules Governing Use**

The use of the Internet is a privilege, not a right, and inappropriate use will result in cancellation of Internet privileges and/or disciplinary action up to and including termination of employment or expulsion of students. All staff and students must abide by the generally accepted rules of Network etiquette, including, but not limited to, the following:

- Be polite. Do not be abusive in messages to others. Always use appropriate language. Profanity, vulgarities, or other inappropriate language is prohibited. Illegal activities are strictly forbidden.
- Documents may not include a person's social security number or any other personally identifiable information that may lead to the identity of one's self or others. For example, do not reveal personal home addresses or phone numbers to others.
- No staff or student pictures (video or still) or audio clips will be published. Posting of photos and other personally identifiable information may violate School policy as well as State and Federal law.
- No original student work will be published without written permission from the student's parent or guardian.
- Users have no expectation of privacy in Electronic mail. People who operate the Network have access to all mail. Messages relating to or in support of illegal or inappropriate activities will be reported to the appropriate authorities.
- Do not disrupt, harass, annoy, or discriminate against other users.
- All communications and information accessible via the Network should be assumed to be private property. Always cite all quotes, references, and sources.
- Never access inappropriate or restricted information, such as pornography or other obscene materials, or other information not directly related to the educational purposes for which access is being provided. Restricted information includes obscene, libelous, indecent, vulgar, profane, or lewd materials; advertisements for products or services not permitted to minors by law, materials whose content advocates and supports violence and/or the harassment of others; and other materials which may cause a substantial disruption of the academic environment in the sole discretion of the administration.
- All subject matter on School Web pages shall relate to administration, programs, curriculum, instruction, School-authorized activities, or to the School.
- Neither students nor staff may publish personal home pages as part of a School Web site or home pages for other individuals or organizations not directly affiliated with the School.
- Vandalism is prohibited and will result, at a minimum, in cancellation of privileges and at the maximum, termination of employment or expulsion of students. Vandalism includes any malicious attempt to harm or destroy data of another user, Internet, or other Networks that are connected to any of the Internet infrastructures. Vandalism also includes, but is not limited to, the uploading or creation of computer viruses, deletion or alteration of other user files or application, removing protection from restricted areas, or the unauthorized blocking of access to information, application, or areas of the Network.
- All users should remain on the Network only as long as necessary to complete their work, so that other individuals will have equal opportunities to access the Internet.
- All users should use the Internet only for research and academic reasons. Users may not use the Network for financial or commercial gain or for personal purchases or trading.
- All pages on the School's server(s) are property of the School.

- Always follow the instructions of the supervising staff members.
- Do not share passwords. The only person who should ever use an account is the person to whom it belongs.
- Adhere to "public performance," not just "fair use" copyright laws on web pages.

The following list represents some of the inappropriate uses, which are not permitted by the School but no means is this list intended to be exhaustive:

- Commercial advertising, fund-raising, or unethical/illegal solicitation.
- Accessing a file or Web site that contains pornographic or obscene pictures, videos, stories, or other material, making copies of such material, or distributing or exposing others to such material.
- Using copyrighted material without permission.
- Sending messages or materials that are obscene, profane, racist, sexist, inflammatory, threatening, or slanderous toward others.
- Creating and/or placing a computer virus/worm on the Network or any workstation.
- Sending messages or information with someone else's name on it or misrepresenting the source of information.
- Sending or receiving messages or information that is inconsistent with the school's conduct code or encourages and/or assists others to violate that code.
- Requesting or distributing addresses, home phone numbers, or other personal information.
- Sending chain letters or engaging in "spamming" (sending annoying, unnecessary or unsolicited messages to large numbers of people.)
- Purchasing something which requires a credit card number or other payment Network or obligates a student or school to provide payment to another party.
- Accessing, attempting to access, and /or altering information in restricted areas of any Network.
- Downloading or loading any software applications without permission from the building Network administrator or Network administrator.
- Violating the confidentiality rights of other users on any Network.
- Failing to report abuses or other conditions that may interfere with the appropriate and efficient use of School's resources.
- Using School's technology resources in order to create electronic forgery.
- Using scanners for any purpose other than School business or educational purposes.
- May not access chat rooms unless participating in an educational chat room while under a teacher's supervision (for students) or approved by supervisor (for staff).
- Prohibiting the usage of video/digital cameras for any purpose other than supporting the School's mission.

Users are required to report any of the following to his/her teacher, supervisor of the building Network administrator as soon as the following are discovered:

- Any messages, files, Web sites, or user activities that contain materials that are in violation of this policy.
- Any messages, files, Web sites, or user activities that solicit personal information, such as an address, phone number, about the user or someone else, or request a personal contact with the user or another user.

- Attempts by any user to abuse or damage the Network or violate the security of the Network and its sources.
- Any illegal activity or violation of school policy.
- Any error messages or problems that indicate that the Network is not working properly.

## **15.4 Penalties for Improper Use**

An employee who violates the terms of this administrative rule or otherwise misuses 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 also will be subject to cancellation over a period of time as determined by the Administration. Students who violate the terms of this administrative rule or who otherwise misuse their access to the Internet also will be subject to disciplinary action as seen appropriate by the principal and Administration, up to and including expulsion. Internet access privileges also may be canceled over a period of time as determined by the administration. Violations of the laws of the United States or the State of Ohio also may subject the user 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.

## **15.5 Warranty**

The School makes no warranties of any kind, whether express or implied, for the service it is providing. The School 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 Network's negligence, user errors, or omissions. Use of any information obtained via the Internet is at the user's own risk. The School specifically denies any responsibility for the accuracy or quality of information obtained through its services.

## **15.6 Security**

Security on any computer Network is a high priority, especially when the Network involves many users. If you believe you have identified a security problem on the Network, you must notify a staff member, Network Administrator, Network Analyst or Director of Technology. Do not demonstrate the problem to other users. Attempts to log on to any Network as a Network administrator will result in cancellation of user privileges and other disciplinary action. Any user identified as a security risk or having a history of problems with other computer Networks may be subject to severe restriction or cancellation of privileges. Abusers agree to accept repair assessment charges for damage or intentional misuse of the Network.

## **15.7 User Privacy**

The School 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.

## **15.8 School Policies**

All documents on the School's server(s) must conform to School policies and regulations, as well as established school offices. Persons developing or maintaining Web documents are responsible for complying with these and other policies. Some of the relevant issues and related School policies include the following:

- Electronic transmission of materials is a form of copying. As specified in School policy, no unlawful copies of copyrighted materials may be knowingly produced or transmitted via the School's equipment, including its Web server(s).
- Documents created for the Web and linked to School Web pages will meet the criteria for use as an informational, administrative or instructional resource.
- Any links to School Web pages that are not specifically curriculum related will meet the criteria established in the School Internet Authorized Use Policy. 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, nonprofit, and non-discriminatory. Web page links may not include entities whose primary purpose is commercial or political advertising.
- All communications via School Web pages will comply with the School Internet Authorized Use policy and the School Code of Conduct policy. Offensive behavior that is expressly prohibited by this policy includes any advocacy of, support for, or actual religious, racial, and sexual harassment and/or violence.
- Any student information communicated via School Web pages will comply with School policies on Data Privacy and Public Use of School Records.

## **16. Other**

Given the rapid change in technology, some of the technical standards outlined in this policy may require change throughout the year. Such changes will be made by the School Network Specialist with approval of the Chief Academic Officer. This Web page policy may be updated on an annual basis, or more frequently if required. Users agree that they will be bound, after reasonable notice, by such updates as if they were a part of the original policy.

## **17. Age Appropriate Summaries of This Policy**

School personnel may create age appropriate summaries of this policy to enhance student understanding of its requirements. The student's parents, however, are primarily responsible for reviewing this Policy with the student to ensure the student is aware of its requirements.



## 18. Code of Conduct – Your copy

This Code of Conduct applies to all users of these technology resources. Honesty, integrity, and respect for the rights of others should be evident at all times. Photographs may only be permitted with current, signed state department of education photo release on file. Students will not be identified by name in conjunction with a recognizable picture. Students will only be identified by first names.

The technology user is held responsible for his/her actions and activities. Unacceptable uses of the Network will result in disciplinary action including possible revocation of these privileges.

Directions: After reading the Metro Early College High School Code of Conduct and Terms and Conditions, please read and fill out the appropriate portions of the following contract completely and legibly. Please return this contract to your Center Coordinator or school administrator.

### USER (Student or Staff) TECHNOLOGY CONTRACT

I have read the Acceptable Use Policy. I understand and will abide by the regulations. I understand misuse is unethical and illegal. Should I commit any violation, my access privileges may be revoked and disciplinary action will be taken. A signed copy of this document must be on file with the administration.

User Name (please print) \_\_\_\_\_

User Signature: \_\_\_\_\_

Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

### PARENT TECHNOLOGY CONTRACT

As the parent or guardian of this student, I have read the Terms and Conditions of the Acceptable Use Policy. I understand that this access is designed for educational purposes and Educational Council School has taken available precautions to monitor student access. However, I also recognize it is impossible for School to restrict all controversial materials, and I will not hold them responsible for the materials acquired on the Network. I hereby give my permission for my child to have school use of technology including the Internet.

Parent or Guardian (please print): \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

Daytime Phone Number: \_\_\_\_\_

Evening Phone Number: \_\_\_\_\_

## 19. Signature – Code of Conduct

This Code of Conduct applies to all users of these technology resources. Honesty, integrity, and respect for the rights of others should be evident at all times. Photographs may only be permitted with current, signed state department of education photo release on file. Students will not be identified by name in conjunction with a recognizable picture. Students will only be identified by first names.

The technology user is held responsible for his/her actions and activities. Unacceptable uses of the Network will result in disciplinary action including possible revocation of these privileges.

Directions: After reading the Metro Early College High School Code of Conduct and Terms and Conditions, please read and fill out the appropriate portions of the following contract completely and legibly. Please return this contract to your Center Coordinator or school administrator.

### USER (Student or Staff) TECHNOLOGY CONTRACT

I have read the Acceptable Use Policy. I understand and will abide by the regulations. I understand misuse is unethical and illegal. Should I commit any violation, my access privileges may be revoked and disciplinary action will be taken. A signed copy of this document must be on file with the administration.

User Name (please print) \_\_\_\_\_

User Signature: \_\_\_\_\_

Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

### PARENT TECHNOLOGY CONTRACT

As the parent or guardian of this student, I have read the Terms and Conditions of the Acceptable Use Policy. I understand that this access is designed for educational purposes and Educational Council School has taken available precautions to monitor student access. However, I also recognize it is impossible for School to restrict all controversial materials, and I will not hold them responsible for the materials acquired on the Network. I hereby give my permission for my child to have school use of technology including the Internet.

Parent or Guardian (please print): \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

Daytime Phone Number: \_\_\_\_\_

Evening Phone Number: \_\_\_\_\_