Cleveland Metropolitan School District
Technology Acceptable Use Policy for Students

Before using technology within the Cleveland Metropolitan School District, all students must read and understand this acceptable use policy. Additionally, by using any school technology a student is agreeing to this policy whether or not it has been read and understood by the student.

1.0 Overview

The Cleveland Metropolitan School District (herein "the District") provides technology to the classroom to support learning. The use of these devices and the networks they are connected to shall be consistent with the curriculum adopted by the District and/or activities required to support instruction or school operations.

Effective security requires a team effort involving the participation and support of every District student and worker. Therefore it is the responsibility of every student to know this policy and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of technology at the District. Inappropriate use seriously impacts the learning process, exposes students to objectionable matter, and/or may present legal issues.

3.0 Scope

This policy relates to all technology equipment owned by the District or utilized on District property.

4.0 Policy

4.1 Privileges and Privacy

- When using District technology, students shall have no expectation of privacy and will give up all rights of privacy under any law or constitution. Additionally, students will consent to monitoring of their activity and if necessary seizing of the District technology assets and data without warning, prior consent or notice by either school officials or law enforcement agencies.
- Students shall not hold the District liable for any damage to assets or data due to harmful programs or viruses that may extend through the technology.
- The District provides access to the internet, but does not endorse content found on the internet.

4.2 General Use and Ownership Match

- Technology is made available to students to support the educational process.
- For security and network maintenance purposes, authorized individuals within the District may monitor equipment, systems and network traffic at any time.
- The District reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy

4.3 Security and Proprietary Information

- Students may only access information and/or computer systems to which they are authorized and that they need for their assignments.
- Students must secure their electronic data. Sensitive files must be saved to a secure location such as the individual's home directory when available (accessed via My Documents for non-laptop users).
- Students may not unlock computers from their security devices or remove computers from any District premises without the written permission from the District's MIS department.
- Students may not remove inventory markings or tags from computers or other technical equipment.
- Students may not disable or modify security setting or measures.
- Keep passwords secure and do not share accounts. Students with network accounts are responsible for the security of their passwords and accounts.
- Students must use extreme caution when opening email attachments received from unknown senders as they may contain viruses that may harm district information.

4.4 Unacceptable Use

The following activities are, in general, prohibited. Under no circumstances is a student of the District authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing District owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the District.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the District or the end user does not have an active license in the District's name is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The

appropriate management should be consulted prior to export of any material that is in question.

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others.
- Using a District computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any District account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee/student/user is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Executing any form of network monitoring which will intercept data not intended for the student, employee or other user's computing asset, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Internet Activities

The District uses internet filtering software to protect its network and prevent students, employees or other users from viewing undesirable sites. This filtering software is required by law (Child Internet Protection Act) as a means to protect the District's students. At no time is any District student permitted to circumvent this software to access a denied site. Other prohibited activities include:

- Utilizing internet "proxy" sites to circumvent internet filtering software and filtered sites
- Accessing profane or obscene material, material suggesting illegal acts and/or material advocating violence or discrimination
- Posting personal contact information
- Agreeing to meet someone online
- Using obscene, profane, lewd, vulgar, inflammatory or threatening language
- Posting false or defamatory information
- Plagiarizing information found on the internet

Email and Communications Activities

While not all students have District-assigned email accounts, students may have personal email accounts (Gmail, Hotmail, Yahoo, etc.) that they can access through the District's network and internet connection. The District cannot access, review, copy or delete any such messages sent, received or stored on the external email systems. Therefore students are expected to adhere fully to the acceptable and unacceptable uses as outlined here.

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment or cyberbullying via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within the District's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the District or connected via the District's network.

5.0 Enforcement

Any student found to have violated this policy will result in cancellation of technology privileges, possible discipline, and/or possible juvenile or criminal court prosecution.

6.0 Revision History

7.0 Legal References

- H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000
- 47 U.S.C. 254(h), (1), Communications Act of 1934, as amended
- 20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended
- 18 U.S.C. 2256
- 18 U.S.C. 1460
- 18 U.S.C. 2246

Student Non-Consent Form

Complete this form **only if you disagree** with the rules regarding internet usage stated in the Cleveland Metropolitan School District's Technology Acceptable Use Policy. Students who complete this form must hand it into the school principal so that internet privileges can be revoked for that student. All other rules pertaining to District technology use, not including the internet, still apply.

.

I do not agree with the rules regarding internet usage as stated in the District's Technology Acceptable Use Policy. I consent to being banned from accessing the internet with District technology assets.

_____ _____
Student Signature Date

_____
Student Name (printed)

I do not agree with the rules regarding internet usage as stated in the District's Technology Acceptable Use Policy. I consent to my student being banned from accessing the internet with District technology assets.

_____ _____
Parent/Legal Guardian Signature Date

_____
Parent/Legal Guardian (printed)

For CMSD MIS Internal Use Only

All forms should be returned to the principal's office of the school and forwarded to MIS' help desk.

_____ _____ _____
Date Received Date Completed Initials