# COMPUTER/ONLINE SERVICES
(Acceptable Use and Internet Safety for Staff)

## I. SCOPE AND PURPOSE

This policy applies to all staff required/authorized to use or have access to the District's Technology Resources.

The District provides access to technology in order to enhance the instructional program, as well as the efficiency of the District. The Board recognizes that careful planning is essential to ensure the successful, equitable and cost-effective implementation of technology-based materials, equipment, systems and networks.

This policy is established to promote the use of Technology Resources in a manner that leads to a safe and worthwhile educational experience for all. The use of CMSD's Technology Resources is a necessary, innate element of the District's educational mission and vision. Technology is provided to students and staff as a privilege, not a right.

Utilization of the District's Technology Resources by staff must be in support of and consistent with the educational objectives of the District. When utilizing the network, all staff must adhere to the provisions of this policy, and other local, state and federal laws.

Computers and use of the District network or online services support learning and enhance instruction, as well as assist in administration. For purposes of this policy the District's Technology Resources include the District network or online services as well as District-owned desktop computers, laptops, tablets and other mobile computing devices.

All Technology Resources are to be used in a responsible, efficient, ethical and legal manner. Failure to adhere to this policy and the guidelines below may result in the revocation of the user's access privilege.

## II. DEFINITIONS

**Account.** For this policy, an "Account" is defined as any directory services account or another set of credentials consisting of a unique username and password that are collectively designed to authenticate the user's identity to provide access to CMSD Technology Resources.

**Parent.** For this policy, a "Parent" is defined as a natural or adoptive parent or other person acting in the capacity of a parent (step-parent, grandparent, guardian, etc.).

**Staff Member**. For this policy, a "Staff Member" is defined as any employee of CMSD, any contractor employed by a company that is providing paid services to CMSD, or any employee or contractor of a charter school under the supervision of CMSD.

**Student**. For this policy, a "Student" is defined as any individual enrolled in a class at any CMSD school or CMSD supervised charter school.

**Technology Resource(s).** For this policy, a "Technology Resource(s)" is defined as any Local Area network; Wide Area Network; Internet or any telecommunications service whether wired or wireless, that is used to access the Internet or any information source that is, or is not owned or controlled by CMSD; or any computing device, regardless of operating system or form factor.

**Visitor.** For this policy a "Visitor" is defined as any non-employee of CMSD that is accessing any technology resource within any facility that is owned by CMSD or occupied and used by CMSD staff members.

**Users.** For this policy, a User is defined as an individual or a collective group that is comprised of Students, Staff Members and Visitors.

## III. AUTHORIZATION FOR USE

Use of the District's Technology Resources sources will be permitted upon submission and approval of authorization form(s) by staff members and visitors.

Employees and other users must sign and return the authorization form(s) to the Chief Information Officer (CIO) or designee.

These policies and regulations also apply to use of District-owned devices, or accessing of District intranet off District property.

Violations of the terms and conditions stated in the authorization agreement may result in revocation of the user's access privileges and/or disciplinary action up to and including termination

## IV. ACCEPTABLE USE

Examples of acceptable use includes but not limited to the following:

- Conducting research in furtherance of District or educational objectives.
- Communicating broadly and effectively.
- Accessing and publishing appropriate data, information and resources.
- Participating in collaborative efforts.

## V. PROHIBITED USE

Prohibited uses of the computer/network include but are not limited to:

- violating the conditions of State and Federal law dealing with students' and employees' rights to privacy, including unauthorized disclosure, use and dissemination of personal information;

- improperly accessing files, data, of information of others, including reposting (forwarding) personal communication without the author's prior consent;

- granting internet or network access to unauthorized persons, or failing to notify a supervisor or the IT Department if you suspect someone of using your password or credentials;

- displaying, uploading, or otherwise distributing photographs or videos of employees or individuals not affiliated with the District without the individual's prior consent, unless the individual is an historic figure or a public figure;

- using profanity, obscenity or other language that may be offensive to another user or intended to harass, intimidate or bully other users;

- transmitting materials that are offensive, threatening or that otherwise are intended to harass or demean recipients, including jokes that are intended to offend, harass or intimidate or other material which is based on slurs or stereotypes relating to race, gender, ethnicity, age, nationality, religion, sexual orientation or disability;

- using the Internet to create, access, or transmit information that is obscene or vulgar, that advocates dangerous or illegal acts or that advocates violence or hatred toward any group;

- using the network or Internet to send messages relating to or in any way supporting illegal activities such as the sale or use of drugs or alcohol; support of criminal or gang activity; threats, intimidation or harassment of any other person;

- plagiarizing i.e. stealing and passing off the ideas or words of another as one's own without crediting the author;

- engaging in copyright infringement; copying commercial software and/or other material in violation of copyright law (copyrighted materials include, but are not limited to, writings, articles, web pages, designs, music, videos, and software);

- accessing personal social networking websites for noneducational purposes

- using the network for financial gain, for commercial activity or for any illegal activity;

- “hacking” or gaining unauthorized access to other computers or computer systems, or attempting to gain such unauthorized access;

- vandalizing or destroying equipment or deleting computer files;

- accessing and/or viewing inappropriate material, including but not limited to obscene, pornographic or other inappropriate material (staff should notify a supervisor or the IT Department if you receive such material);

- downloading of freeware or shareware programs.

## VI. NETWORK ETIQUETTE

All staff authorized to use the District network are expected to abide by the generally accepted rules of network etiquette. These standards of conduct include, but are not limited to the following:

- Be polite and respectful.
- Use appropriate language. The use of abusive language, profanity, vulgarities or any other inappropriate language is prohibited.
- Harassment is unacceptable and prohibited.
- Cyberbullying is prohibited.
- Staff should not reveal their personal addresses and/or telephone numbers or those of students, other staff or colleagues.
- Note that electronic mail (email) is not guaranteed to be private. Technology coordinators have access to all messages relating to or in support of illegal activities and such activities may be reported to the authorities.
- The network should not be used in such a way that it disrupts the use of the network by others.
- All communications and information accessible via the network should be assumed to be property of the District.
- Users shall not use the system to encourage the use of drugs, alcohol or tobacco nor shall they promote unethical practices or any activity prohibited by law or Board policy.

## VII. REVIEW AND MONITORING

The District reserves the right to monitor, inspect, copy, review and/or store at any time and without prior notice any and all results of usage of computers, network and/or Internet access and any and all information transmitted or received in connection with such usage. This includes information contained in online services provided by the district. All such information shall be and remain the property of the District and users shall have no expectation of privacy regarding such materials. The creator of original works may retain specific rights to use as applicable under U.S. copyright law. Staff shall maintain and protect the confidentiality of any confidential information housed, processed or maintained by the District. This includes but is not limited to account information, passwords and personal information.

Because access to online services provides connections to other computer systems located all over the world, users (and parents of users who are under 18 years old) must understand that neither the school nor the District can control the content of the information available on these systems. Some of the information available is controversial and sometimes offensive.

The District does not condone the use of such materials. Employees, students and parents of students must be aware that the privileges to access online services are withdrawn from users who do not respect the rights of others or who do not follow the rules and regulations established. A user's agreement is signed to indicate the user's acknowledgment of the risks and regulations for computer/online services use. The District has implemented technology-blocking measures that protect against access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to the use of computers by minors, harmful to minors. The District has also purchased monitoring devices that maintain a running log of Internet activity, recording which sites a particular user has visited.

## VIII. CHILDRENS' INTERNET PROTECTION ACT

The Children's Internet Protection Act (CIPA) requires school districts that receive federal funds to purchase computers, direct access to the internet under the Elementary and Secondary Education Act or receive universal E-rate service discounts And internet services under the Communications Act to adopt implement and maintain computer use policies to prevent students from viewing objectionable material that address these issues:

.

- Access by minors to inappropriate matter on the Internet and World Wide Web
- Access by both adults and minors to visual depictions that are obscene, child pornography on the Internet and World Wide Web;
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications
- Unauthorized access including "hacking" and other unlawful activities by minors online
- Unauthorized disclosure, use, and dissemination of personal information regarding minors
- Measures designed to restrict minors' access to materials harmful to minors
- Educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

The District will educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response and will develop a program to educate students on these issues.

## IX. SECURITY

Pursuant to CIPA, CMSD uses an Internet Content Filter to prevent all users' access to prohibited material. Bypassing the CMSD content filter without authorization is strictly prohibited. CMSD has procedures in place to evaluate request from users to block or unblock sites as necessary.

The security on CMSD's Networks is a high priority, especially when the telecommunications environment involves many users. To minimize data security issues, Staff are required to follow the following procedures:

- If an internet/network security issue is identified, the user must notify the IT Department (do not try to demonstrate the problem to others.);
- A user with a history of clicking/accessing phishing or malicious emails may be denied access to the District network until he/she has taken an official District offered cyber security class and successfully passed the associated examination(s). The District reserves the right to take further disciplinary actions as described in Section XII – Consequence for Improper Use contained herein.
- Do not conduct mass e-mailing of unsolicited or unwanted messages ("spamming"), including text, software, video images, and graphics.
- Do not attempt to log on as a system administrator. This action will result in cancellation

of privileges.

- Do not use anonymous proxies to circumvent District implemented content filtering.
- Do not knowingly or inadvertently load or create a computer virus or load any software that destroys files and programs, confuses users, or disrupts the performance of the system.
- Do not install third party software without the consent of your assigned administrator.
- Do not share your passwords.
- Do not use another person's accounts or passwords.
- Technology protection measures may be disabled by an authorized person. This will be done only by Information Technology Management (ITM) during adult computer usage to enable internet access for research or other lawful purposes.
- Do not participate in hacking/cracking activities or any form of unauthorized access to other computers, networks, or information systems.

## X. ATTORNEY-CLIENT PRIVILEGED COMMUNICATIONS

Some of the messages sent, received or stored on the District e-mail system will constitute confidential, privileged communications between the District and either its internal or external attorneys. Upon receipt of a message either from or to counsel, the message content should not be forwarded to others inside the District without counsel's authorization. Such messages or their contents should never be forwarded to any outsiders. Violation of this policy may result in discipline up to and including termination.

## XI. CONFIDENTIALITY OF STUDENT AND PERSONAL INFORMATION

Personally identifiable information concerning students may not be disclosed or used in any way on the internet without the permission of a parent or guardian or, if the student is 18 or older, the permission of the student himself/herself. Users should also never provide private confidential information about themselves or others on the internet, such as credit card or Social Security Numbers.

## XII. CONSEQUENCE FOR IMPROPER USE

The act of signing the acceptable use policy authorization agreement and/or accessing the Internet through the District's network signifies that the staff member will comply with the provisions of this policy. Inappropriate use by a staff member may result in the staff member's access privileges being taken away or other disciplinary action up to and including termination being taken by the District.

[Adoption date: February 20, 2018]

LEGAL REFS.: U.S. Const. Art. I, Section 8
Family Educational Rights and Privacy Act; 20 USC 1232g et seq.
Children's Internet Protection Act; 47 USC 254 (h)(5)(b)(iii); (P.L. 106-554,

HR 4577, 2000, 114 Stat 2763)
ORC 3313.20
3319.321

CROSS REFS.: AC, Nondiscrimination
ACA, Nondiscrimination on the Basis of Sex
ACAA, Sexual Harassment
EDEB, Bring Your Own Technology (BYOT) Program
GBCB, Staff Conduct
GBH, Staff-Student Relations (Also JM)
IB, Academic Freedom
IIA, Instructional Materials
IIBH, District Websites
JFC, Student Conduct (Zero Tolerance)
JFCF, Hazing and Bullying (Harassment, Intimidation and Dating Violence)
Staff Handbooks
Student Handbooks

***THIS IS A REQUIRED POLICY***