STUDENT EDUCATION TECHNOLOGY ACCEPTABLE USE AND SAFETY

Source: P.L. 106-554, Children's Internet Protection Act of 2000
P.L. 110-385, Title II, Protecting Children in the 21st Century Act
18 U.S.C. 1460
18 U.S.C. 2246
18 U.S.C. 2256
20 U.S.C. 6777, 9134 (2003)
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)
47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)
47 C.F.R. 54.520

Technology has fundamentally altered the ways in which information is accessed, communicated, and transferred in society. As a result, educators are continually adapting their means and methods of instruction, and the way they approach student learning, to incorporate the vast, diverse, and unique resources available through the Internet. The Board provides Education Technology so that students can acquire the skills and knowledge to learn effectively and live productively in a digital world. The Board of Directors provides students with access to the Internet for limited educational purposes only and utilizes online educational services to enhance the instruction delivered to its students. The Academy's Internet system does not serve as a public access service or a public forum, and the Board imposes reasonable restrictions on its use consistent with tis limited educational purpose.

This policy and its related administrative guidelines and the Student Code of Conduct govern students' use of the Academy's computers, laptops, tablets, personal communication devices (as defined by Policy 5136), network, and Internet connection and online educational services ("Education Technology" or "Ed-Tech"). The due process rights of all users will be respected in the event there is a suspicion of inappropriate use of the Education Technology. Users have no right or expectation to privacy when using the Ed-Tech (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity while on the network and Internet).

This policy and its related administrative guidelines and the Student Code of Conduct also govern students' use of their personal communication devices (that is, according to Policy 5136, computers, laptops, tablets, e-readers, cellular/mobile telephones, smartphones, and any other web-enabled device), when connected to the Academy's network, the Academy's Internet connection, and online educational services ("Education Technology" or "Ed-Tech"). The due process rights of all users will be respected in the event there is a suspicion of inappropriate use of the Education Technology. Users have no right or expectation to privacy when using the Ed-Tech (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity while on the network and Internet).

First, and foremost, the Board may not be able to technologically limit access to services through the its Educational Technology to only those services and resources that have been authorized for the purpose of instruction, study and research related to the curriculum. Unlike in the past when educators and community members had the opportunity to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to adopted procedures and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them), access to the Internet, because it serves as a gateway to any publicly available file server in the world, opens classrooms and students to electronic

information resources that may not have been screened by educators for use by students of various ages.

Pursuant to Federal law, the Board has implemented technology protection measures which protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act. At the discretion of the Board or the School Leader, the technology protection measures may be configured to protect against access to other material considered inappropriate for students to access. The Academy also utilizes software and/or hardware to monitor online activity of students to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. However, the Board is cognizant of the fact that such software and/or hardware is not perfect and relies on students to self-police (and immediately cease viewing) online activity that would otherwise be in conflict with these policies and to immediately report such to the School Leader. The Educational Service Provider may temporarily or permanently unblock access to websites or online education services containing appropriate material, if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures.

Parents/guardians are advised that a determined user may be able to gain access to services on the Internet that the Board has not authorized for educational purposes. In fact, it is impossible to guarantee students will not gain access through the Internet to information and communications that they and/or their parents/guardians may find inappropriate, offensive, objectionable or controversial. Parents/Guardians assume risks by consenting to allow their child to participate in the use of the Internet. Parents/Guardians of minors are responsible for setting and conveying the standards that their children should follow when using Education Technology. The Board supports and respects each family's right to decide whether to apply for independent student access to the Education Technology.

The technology protection measures may not be disabled at any time that students may be using the Education Technology, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. Any student who attempts to disable the technology protection measures will be subject to discipline.

The Educational Service Provider is directed to prepare procedures which address students' safety and security while using e-mail, chat rooms and other forms of direct electronic communications, and prohibit disclosure of personal identification information of minors and unauthorized access (e.g., "hacking"), cyberbullying and other unlawful or inappropriate activities by minors online.

Pursuant to Federal law, students shall receive education about the following:

A. safety and security while using e-mail, chat rooms, social media, and other forms of direct electronic communications;

B. the dangers inherent with the online disclosure of personally identifiable information;

C. the consequences of unauthorized access (e.g., "hacking") cyberbullying and other unlawful or inappropriate activities by students online, and

D. unauthorized disclosure, use, and dissemination of personal information regarding minors.

The Board directs the Educational Service Provider to implement procedures regarding the appropriate use of technology and online safety and security as specified above. Furthermore, the Educational Service Provider will implement monitoring procedures for the online activities while students are at school.

Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions; or use of specific monitoring tools to review browser history and network, server, and computer logs.

The Educational Service Provider is responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying procedures. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of the Education Technology. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. All Internet users (and their parents if they are minors) are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying procedures.

Students may be assigned a school email account that they are required to utilize for all Academy-related electronic communications, including those to staff members and individuals and/or organizations outside the Academy with whom they are communicating for Academy-related projects and assignments. Further, as directed and authorized by their teachers, they shall use their Academy-assigned email account when signing up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the student for educational purposes.

Students and staff members are responsible for good behavior on the School's computers/network and the Internet just as they are in classrooms, school hallways, and other school premises and school sponsored events. Communications on the Internet are often public in nature. General school rules for behavior and communication apply. The Board does not sanction any use of the Education Technology that is not authorized by or conducted strictly in compliance with this policy and its accompanying procedures.

Students shall not access social media for personal use from the School's network, but shall be permitted to access social media for educational use in accordance with their teacher's approved plan for such use.

Users who disregard this policy and its accompanying procedures may have their use privileges suspended or revoked, and disciplinary action taken against them. Users of the Board's Education Technology are personally liable, both civilly and criminally, for uses of the Education Technology not authorized by this Board policy and its accompanying procedures. The Board designates the Educational Service Provider as the persons responsible for initiating, implementing, and enforcing this policy and its accompanying procedures as they apply to the use of the Academy's Education Technology and the Internet for instructional purposes.

Revised 1/11/10; 7/11/11; 9/13/12; 3/18/15

STAFF EDUCATION TECHNOLOGY ACCEPTABLE USE AND SAFETY

Source: P.L. 106-554, Children's Internet Protection Act of 2000
P.L. 110-385, Title II, Protecting Children in the 21st Century Act
18 USC 1460
18 USC 2246
18 USC 2256
20 USC 6777, 9134 (2003)
20 USC 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)
47 USC 254(h), (1), Communications Act of 1934, as amended (2003)
47 C.F.R. 54.520

Technology has fundamentally altered the ways in which information is accessed, communicated, and transferred in society. As a result, educators are continually adapting their means and methods of instruction, and the way they approach student learning, to incorporate the vast, diverse, and unique resources available through the Internet. The Board of Directors provides staff with access to the Internet for limited educational purposes only and utilizes online educational services to enhance the instruction delivered to its students and to facilitate the staff's work. The Academy's Internet system does not serve as a public access service or a public forum, and the Board imposes reasonable restrictions on its use consistent with its limited educational purpose.

This policy and its related administrative guidelines and any applicable employment contracts and collective bargaining agreements govern the staffs' use of the Academy's computers, laptops, tablets, personal communication devices (as defined by Policy 7530.02), network and Internet connection and online educational services ("Education Technology" or "Ed-Tech"). The due process rights of all users will be respected in the event there is a suspicion of inappropriate use of the Education Technology. Users have no right or expectation to privacy when using the Ed-Tech Technology. Users have no right or expectation to privacy when using the Ed-Tech (including, but not limited to, privacy in the content of their persona files, e-mails, and records of their online activity while on the network and Internet).

Staff are expected to utilize Education Technology in order to promote educational excellence in our schools by providing students with the opportunity to develop the resource sharing, innovation, and communication skills and tools that are essential to both life and work. The Board encourages the faculty to develop the appropriate skills necessary to effectively access, analyze, evaluate, and utilize these resources in enriching educational activities. The instructional use of the Internet and online educational services will be guided by the Board's policy on Instructional Materials.

The Internet is a global information and communication network that brings incredible education and information resources to our students. The Internet connects computers and users in the Academy with computers and users worldwide. Through the Internet, students and staff can access relevant information that will enhance their learning and the education process. Further, the Education Technology provides students and staff with the opportunity to communicate with other people from throughout the world. Access to such an incredible quantity of information and resources brings with it, however, certain unique challenges and responsibilities.

First, and foremost, the Board may not be able to technologically limit access to services over its Education Technology to only those services and resources that have been authorized for the purpose of instruction, study and research related to the curriculum. Unlike in the past when educators and community members had the opportunity to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to

adopted procedures and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them), access to the Internet, because it serves as a gateway to any publicly available file server in the world, opens classrooms and students to electronic information resources that may not have been screened by educators for use by students of various ages.

Pursuant to Federal law, the Board has implemented technology protection measures, which protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act. At the discretion of the Board or Educational Service Provider, the technology protection measures may also be configured to protect against access to other material considered inappropriate for students to access. The Board utilizes software and/or hardware to monitor online activity of staff members to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. However, the Board is cognizant of the fact that such software and/or hardware is not perfect and relies on Staff members to self-police (and immediately cease viewing) online activity that would otherwise be in conflict with these policies and to immediately report such to the School Leader.

The technology protection measures may not be disabled at any time that students may be using the Education Technology, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. Any staff member who attempts to disable the technology protection measures will be subject to disciplinary action, up to and including termination.

The Educational Service Provider or School Leader may temporarily or permanently unblock access to websites containing appropriate material, if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures. The Educational Service Provider or School Leader may also disable the technology protection measures to enable access for bona fide research or other lawful purposes.

The Educational Service Provider is directed to prepare procedures which address students' safety and security while using e-mail, chat rooms and other forms of direct electronic communication, and prohibit disclosure of personal identification information of minors and unauthorized access (e.g., "hacking"), cyberbullying and other unlawful or inappropriate activities by minors online. Staff members are reminded that personally identifiable student information is confidential and may not be disclosed without prior written parental permission.

The Board directs the Educational Service Provider to initiate professional development programs in accordance with the provisions of law and this policy. Training shall include:

A. the safety and security of students while using e-mail, chat rooms, social media and other forms of direct electronic communications;

B. the inherent danger of students disclosing personally identifiable information online;

C. the consequences of unauthorized access (e.g., "hacking"), cyberbullying and other unlawful or inappropriate activities by students or staff online; and

D. unauthorized disclosure, use, and dissemination of personal information regarding minors.

Furthermore, the Board directs the Educational Service Provider to cause to provide instruction for students regarding the appropriate use of technology and online safety and security as specified above, and the Educational Service Provider will implement monitoring procedures for the online activities while students are at school.

Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions; or use of specific monitoring tools to review browser history and network, server, and computer logs.

The disclosure of personally identifiable information about students online is prohibited.

Educational Service Provider is responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying procedures. The Board expects that guidance will be provided and instruction offered to students in the appropriate use of the Education Technology. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. All Internet users are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying procedures.

Staff will be assigned an Academy email address that they are required to utilize for all Academy-related electronic communications, including those to students and their parents and other staff members.

With prior approval from the Educational Service Provider or School Leader, staff may direct students who have been issued Academy-assigned email accounts to use those accounts when signing up/registering for access to various online educational services including mobile applications/apps that will be utilized by the students for educational purposes under the teacher's supervision.

The Board expects all Academy personnel to be responsible for good behavior when using the Academy's Education Technology just as in classrooms, school hallways, and other school premises and school sponsored events. Communications on the Internet are often public in nature.

Staff members shall not access social media for personal use on the School's network, and shall access social media for educational use only after submitting a plan for that educational use and securing the School Leader's approval of that plan in advance.

General Academy rules for behavior and communication apply. The Board does not sanction any use of the Internet that is not authorized by or conducted strictly in compliance with this policy and its accompanying procedures. Users who disregard this policy and its accompanying procedures may have their use privileges suspended or revoked, and disciplinary action taken against them. Users of the Academy's technology are personally responsible and liable, both civilly and criminally, for uses of the Education Technology not authorized by this policy and its accompanying procedures.

Social Media Use

Personal or private use of social media, such as Facebook, Twitter, MySpace, blogs, etc., may result in unintended consequences. While the Board respects employees First Amendment rights, those rights do not include permission to post inflammatory comments that could compromise the School's Mission, undermine staff relationships, or cause a substantial disruption to the school environment. This warning includes School personnel online conduct that occurs off school property, including from the School's personal or private computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

In addition, Federal and State confidentiality laws forbid schools and School employees from using or disclosing student education records without parental consent. See Policy 8330. Education records include a wide variety of information; posting personally identifiable information about students is not permitted. School personnel who violate State and Federal confidentiality laws or privacy laws related to the disclosure of confidential employee information may be disciplined.

The Board designates the Educational Service Provider as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying procedures as they apply to the use of the Academy's Education Technology.

Adopted 1/11/10
Revised 7/11/11; 9/13/12; 3/18/15

ACCEPTABLE USE POLICY

Our Goal: A safe, sensible approach

As a student of this school:

A. You must never reveal personal information, your name, where you live, your parents' names, your telephone number, or where you go to school.

B. Don't send pictures of yourself or your family through the Internet.

C. Always tell your teacher about any web site that makes you feel uncomfortable, or any communication that uses threatening or bad language.

D. Remember that people on the Internet can be anyone, anywhere. Be careful to protect yourself, your fellow students, and your family.

E. Only visit web sites that are appropriate for school. If you see something that you know isn't right, back out of it immediately or shut down your browser.

F. Make good choices. Do not accept product offers or other opportunities to send you information through the Internet without your parents' specific approval.

G. Avoid chat rooms. They are not allowed, ever.

H. Never send or receive e-mail messages without permission from school authorities. If the principal or computer instructor didn't say you are allowed e-mail privileges, they are expressly forbidden.

I. Don't agree to meet someone you've met on the Internet. Tell a grownup about anyone who even suggests this.

J. Follow the policies in the written Internet contract which you and your parents signed at the beginning of the year.

Consequences

The key to a successful Internet safety system is adult supervision. Nothing can replace the influence of a vigilant teacher. Students who knowingly violate the recommended guidelines will lose their Internet or computer privileges, and in extreme cases a parent conference must be scheduled.

The school has filtering software that monitors and blocks inappropriate web usage. The technology coordinator, in cooperation with the principal, will work to prohibit access to sites that are not appropriate, such as game or entertainment sites with no academic value. Filtering software is not perfect, but it is an important part of our overall program.

Purpose

This policy establishes rules governing employee use, at school, business or affiliated sites, of the Cesar Chavez Academy provided Internet resources. The Internet is a powerful communications tool and a valuable source of information about vendors, customers, competitors, technology, and new products and services. Email and Internet access must be used in a manner that is consistent with the Cesar Chavez Academy's standards of business conduct. An employee's improper use of Cesar Chavez Academy-provided Internet services can waste time and resources and create legal liability and embarrassment for both Cesar Chavez Academy and the employee. This policy may be changed at any time.

Policy Scope

An Internet service includes, but is not limited to: email, FTP, telnet, web browsing, and Usenet or newsgroups. This policy also applies to any Internet service that is:

A. accessed on or from Cesar Chavez Academy's premises;

B. accessed using company computer equipment or via company-paid access methods; and/or,

C. used in a manner that identifies the individual with the company.

Prohibited Activities

Employees are strictly prohibited from using the Cesar Chavez Academy-provided Internet services for inappropriate use. Inappropriate use includes, but is not limited to any of the following activities:

A. engaging in illegal, fraudulent, or malicious conduct;

B. working on behalf of organizations without any professional or business affiliation with the Cesar Chavez Academy;

C. sending, receiving, or storing offensive, obscene, or defamatory material;

D. sending uninvited email of a personal nature;

E. monitoring or intercepting the files or electronic communications of employees or third parties;

F. obtaining unauthorized access to any computer system;

G. using another individual's account or identify without explicit authorization;

H. attempting to test, circumvent, or defeat security or auditing systems of the Cesar Chavez Academy or any other organization without prior authorization; or,

I. distributing or storing chain letters, jokes, solicitations, offers to buy or sell goods, or other non-business material of a trivial or frivolous nature;

J. transmitting to public bulletin boards, chat rooms, and other public forums, and to individuals or other entities, information about the Cesar Chavez Academy;

K. broadcasting or transmitting inappropriate personal views on business or nonbusiness matters, or representing personal views as those of the Cesar Chavez Academy;

L. gambling or conducting illegal activities; and

M. interfering with the normal operation or performance of the communications systems of the Cesar Chavez Academy.

Personal Use

Internet services are provided by the Cesar Chavez Academy for employees' business use. Very limited or incidental use of Internet services for personal, non-business purposes is acceptable. However, personal use must be infrequent and must not:

A. involve any prohibited activity ;

B. interfere with the productivity of the employee or his or her co-workers;

C. consume system resources or storage capacity on an ongoing basis; or

D. involve large file transfers or otherwise deplete system resources available for business purposes.

Employer Monitoring Rights

Employees should not expect privacy with respect to any of their activities using the Cesar Chavez Academy-provided Internet access or services. The Cesar Chavez Academy reserves the right to review any files, messages, or communications sent, received or stored on the Cesar Chavez Academy's computer systems.

Discipline

Employees violating this policy are subject to discipline, up to and including termination of employment. Employees using the Cesar Chavez Academy's computer system for defamatory, illegal, or fraudulent purposes are also subject to civil liability and criminal prosecution.

PERSONAL INTERNET ACCOUNT PRIVACY - STUDENTS

Reference: Michigan Internet Privacy Information Act, PA 478 of 2012
M.C.L. 37.271 et. seq.

The Academy will not:

A. request a student or prospective student to grant access to, allow observation of, or disclose information that allows access to or observation of the student's or prospective student's personal internet account.

B. expel, discipline, fail to admit, or otherwise penalize a student or prospective student for failure to grant access to, allow observation of, or disclose information that allows access to or observation of the student's or prospective student's personal internet account.

The following definitions shall be used for this policy:

A. "Access information" means user name, password, login information, or other security information that protects access to a personal internet account.

B. "Personal internet account" means an account created via a bounded system established by an internet-based service that requires a user to input or store access information via an electronic device to view, create, utilize, or edit the user's account information, profile, display, communications, or stored data.

C. The Academy may:

1. request or require a student to disclose access information to gain access to or operate any of the following:

   a. An electronic communications device paid for in whole or in part by the Academy.

   b. An account or service provided by the Academy that is either obtained by virtue of the student's admission to the educational institution or used by the student for educational purposes.

2. view, access or utilize information about a student or applicant that can be obtained without any required access information or that is available in the public domain.

Adopted 7/11/13

PERSONAL INTERNET ACCOUNT PRIVACY – STAFF

Reference: Michigan Internet Privacy Protection Act, PA 478 of 2012
M.C.L. 37.271 et. seq.

The Academy will not:

A. request an employee or an applicant for employment to grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal internet account.

B. discharge, discipline, fail to hire, or otherwise penalize an employee or applicant for employment for failure to grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal internet account.

The following definitions shall be used for this policy:

A. "Access information" means user name, password, login information, or other security information that protects access to a personal internet account.

B. "Personal internet account" means an account created via a bounded system established by an internet-based service that requires a user to input or store access information via an electronic device to view, create, utilize, or edit the user's account information, profile, display, communications, or stored data.

C. The Academy may:

1. request or require an employee to disclose access information to the Academy to gain access to or operate any of the following:

   a. An electronic communications device paid for in whole or in part by the employer.

   b. An account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or used for the Academy's business purposes.

2. discipline or discharge an employee for transferring the proprietary or confidential information or financial data to an employee's personal internet account without the Academy's authorization.

3. conduct an investigation or require an employee to cooperate in an investigation in any of the following circumstances:

   a. If there is specific information about activity on the employee's personal internet account, for the purpose of ensuring compliance with applicable laws, regulatory

requirements, or prohibitions against work-related employee misconduct.

b. If the Academy has specific information about an unauthorized transfer of the Academy's proprietary information, confidential information, or financial data to an employee's personal internet account.

4. restrict or prohibit an employee's access to certain websites while using an electronic communications device paid for in whole or in part by the Academy or while using the Academy's network or resources, in accordance with State and Federal law.

5. monitor, review, or access electronic data stored on an electronic communications device paid for in whole or in part by the employer, or traveling through or stored on an Academy's network, in accordance with State and Federal law.

6. screen employees or applicants prior to hiring or to monitor or retain employee communications that is established under Federal law or by a self-regulatory organization, as defined in section 3(a)(26) of the securities and exchange act of 1934, 15 USC 78c(a)(26).

7. view, access or utilize information about an employee or applicant that can be obtained without any required access information or that is available in the public domain.

Adopted 7/11/13