Capital School District

Board of Education Policy

Section: Administration
Title: Acceptable Use and Internet Safety Policy
Policy #: 200-11
Date Approved: 07/18/12
Date Revised: 05/16/12

Purpose:

The Capital School District recognizes that the appropriate use of technology provides students with the best opportunities to prepare them with the skills needed to be competitive within a global society. Through a wide variety of mediums, technology connects students and staff to libraries, online resources, diverse cultural and rich multimedia experiences, and a number of other academic resources around the world. While the benefits of technology far outweigh its potential shortcomings, the manner in which it is used is significant in determining its value. To that end, we are pleased to provide technology resources for student and employee use.

The State of Delaware also provides access to email, content filtering in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA), network access, and other services. As such, employees are required to sign the State of Delaware's Acceptable Use Policy (DTI-0042.02). The Capital School District's Acceptable Use and Internet Safety Policy reaffirms those standards and outlines the guidelines and behaviors that users are expected to follow when using technology resources, as well as expanding on key parts of the State's policy.

Technologies Covered

Capital School District provides and supports a wide array of technologies, including but not limited to desktop computers, mobile computers and devices, interactive white boards, responders, shared storage and online collaborative systems, internet and website services, access to email, data and reporting services, and many others.

The introduction of new technologies occurs continuously within the District. The policies outlined in this document cover the items listed above, as well as any others currently in use and those used in the future. If questions arise regarding the use of a specific technology or the application of these policies, users should contact the Technology Office for clarification with enough time to properly review the request. Until the matter has been resolved, the use of that technology or resource is prohibited.

General Usage

All technologies provided by the district are intended for educational purposes. All users are expected to use good judgment and to follow the guidelines established within this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

- Only Capital School District faculty, staff, students and individuals with written authorization from the appropriate district and state authorities are allowed to use the district's technology systems and resources. The Acceptable Use and Internet Safety Policy must be signed prior to access being granted.

- The use of any technology resources, including any associated activities, may be monitored and any records thereof may be retained indefinitely.
- Users are expected to alert the appropriate district staff immediately of any concerns for safety or security.
- Transmission of any material in violation of any international, national or state law or regulations is prohibited. This includes, but is not limited to, copyrighted materials, threatening or obscene material, harassing material, or material protected by trade secrets.
- Using district resources for commercial activities, product advertisement, or political lobbying is not acceptable.
- Illegal activities are strictly prohibited.
- Excessive personal web browsing is not permitted. Examples of excessive uses include utilizing streaming services such as listening to music or videos not related to one's job duties, playing online games (excluding websites used during instruction), or using an unfair portion of network bandwidth as compared to other users.
- Storing personal files that are not used during instruction, such as music, videos, and pictures on district servers is prohibited. Users should be conscious of the type of space that these files take up, in order to ensure that they are using district resources in the best manner possible.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Users are expected to follow the same rules for good behavior and respectful conduct that they do in person when using district resources, as well as when accessing online resources from outside the district's network or with personal devices.
- Misuse of technology resources and systems can result in disciplinary action.
- Capital School District makes a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from the use of school technologies systems and resources.

Privileges

The use of Capital School District systems and resources is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. Before being approved for access, users must agree to abide to these policies by signing their acknowledgement and agreement to these policies.

Network Etiquette

Users are expected to abide by the generally accepted rules of network etiquette, in that users should always use technology resources, in a courteous and respectful manner. Some recommendations include:

- Do not post anything online that you would not want parents, teachers, or future colleges or employers to see. Once something is online, it's out there—and can sometimes be shared and spread in ways you never intended.
- Recognize that among valuable online content is unverified, incorrect, or inappropriate content. Users should only use trusted academic sources when conducting research via the Internet.

- Be polite. Be aware that emails can sometimes be interpreted differently than when speaking to someone in person. For instance, writing in all caps conveys shouting and is discouraged.
- Sending abusive messages to others in any medium is not acceptable.
- There is no expectation of privacy. Messages relating to or in support of illegal activities, even when created in jest, may be reported to the authorities.
- Users must respect the privacy of others. Revealing the personal home address, phone number of students or colleagues, and other information is prohibited.
- Use appropriate language. Avoid swearing, using vulgarities or any other inappropriate language or symbols.
- Respect the rights of other users by not disrupting the system (e.g. downloading huge files or monopolizing resources, sending unnecessary mass e-mail messages or replying to everyone in an email thread when it would be more appropriate to only respond to the original sender, etc.).

Cyberbullying

Please refer to Board Policy #700-31 Bullying Prevention Policy.

Education, Supervision and Monitoring

It shall be the responsibility of all teachers and technology staff to educate, supervise and monitor appropriate usage of the computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Supervisor of Technology or designated representatives.

Teachers of technology or designated representatives will provide age appropriate training for students who use Capital School District's Internet facilities. The training provided will be designed to promote the district's commitment to:

a. The standards and acceptable use of Internet services as set forth in this Acceptable Use and Internet Safety Policy;
b. Student safety with regard to:
    i. safety on the Internet;
    ii. appropriate behavior while on online, on social networking Web sites, chat rooms; etc.
    iii. cyberbullying awareness and response.
c. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Communication between Students and Staff

Students and staff are expected to interact professionally at all times. Due to the informal nature of some forms of communication, it is recommended that extra steps be taken to avoid even the perception of inappropriate behavior. Emails, online postings, text messages, and other forms are expected to occur transparently, be retained whenever possible, and be limited to official school business. Formal methods (letters, emails) over informal methods (e.g. text messaging) should be used unless one form of communication is clearly more effective. For instance, providing students with a cell phone number for emergencies during a field trip, or informing team members of a last minute change to a practice schedule. If communication occurs that has the potential to be misconstrued as inappropriate, it should be discussed with the school's administrator.

Personal Safety

Users should recognize that technology resources, especially those on the internet, provide many benefits, as well as expose users to certain risks. Information should be guarded carefully, and one should never share personal information, including phone numbers, addresses, social security numbers, birthdays, and so on, without a parent's or adult's supervision and approval. Users should never agree to meet someone they met online in real life without parental permission.

If you see a message, comment, image, or anything else online that makes you uncomfortable or concerned for your or someone else's personal safety, immediately bring it to the attention of an adult (teacher or staff if you are at school; parent if you are at home).

Vandalism

Vandalism is defined as any attempt to harm or destroy data, disrupt network or other services, affect another user's access, or create, upload, or download computer viruses, spyware and malware. Vandals will be subject to cancellation of privileges and may be liable for any direct or indirect damages incurred.

Plagiarism

Plagiarism occurs when someone uses ideas, pictures, and other information without citing the original source or author. While copying an entire paper easily constitutes plagiarism, taking small excerpts out of papers or even accidentally excluding the sources of passages that have been paraphrased can also be in violation of this policy. Even when unintentional, plagiarism is a form of intellectual theft and great care should be taken to avoid it. The best method to avoid plagiarism is to use academic resources and to cite all of the resources that you use within the body of your work.

Web Access/Filtering

Access to internet resources is controlled both by Capital School District, as well as the State of Delaware. State of Delaware network and website filtering ensures compliance with state and federal regulations, such as the Children's Internet Protection Act (CIPA). As required by CIPA and to the extent practical, internet filters shall be used to block access to visual depictions of material deemed obscene, child pornography, or to any material deemed harmful to minors. Additionally, Capital School District reserves the right to add additional layers of protection and filtering. Bypassing any of the safeguards used to protect users, including network filtering by Capital School District and the State, is strictly prohibited. The use of any technology resources, including internet resources, may be monitored and the associated records may be retained indefinitely.

While a significant portion of the information and interaction available to users is consistent with the educational goals of the district, the diversity of a global network will also have material that is not considered to possess an appropriate educational value. Capital School District is using the available resources to ensure that everyone's access is as safe as possible, while still providing access to the academic resources required to advance the needs of our students. If a currently blocked resource should be allowed, users may report the resource to the Technology Office so that it may be properly reviewed. Likewise, if a currently allowed resource is inappropriate, it should be reported as well. At the present time it is impossible to completely restrict access to controversial materials, so students, parents, and staff must work together to ensure appropriate use of these systems.

Email

All district employees will be provided with an email account, including any individuals that communicate on behalf of Capital School District. Any emails relating to school or district business should occur through the email provided by the district. As such, the forwarding of emails to external accounts is not permitted.

While incidental and occasional personal use of email may occur, it must not generate any costs for the district. Any such incidental and occasional use for personal purposes is subject to the provisions of this policy. The mass sharing of jokes, personal stories, chain letters, and so on is prohibited. The emailing and responding to listservs, district distribution lists, and similar technology must be approved by the appropriate district resource prior to doing so.

Users should not attempt to open files or hyperlinks, unless they know that the resource they are attempting to access is secure and appropriate. Users should not provide any usernames and passwords via email, as the Technology Office and other official agencies will not request that information via email. Users are expected to communicate via email in the same appropriate, safe, mindful, courteous manner that they do offline or in person.

Social Media Usage

"Social media" includes all forms of online applications, websites, tools, and platforms that enable communication between users. The specific types of social media change frequently but, as a general matter, include: (a) social-networking sites (e.g., Facebook, MySpace, and LinkedIn) (b) blogs and micro-blogs (e.g. Wordpress, Blogger, Twitter, and Tumblr); and (c) content-sharing sites (e.g. Flickr, YouTube, Vimeo, Scribd). Additionally, comments posted to a website or blog, and other user-generated content are subject to the standards set forth in this policy.

The creation and usage of social media websites for official purposes must be preapproved by the appropriate district resources and administrative access may be required by the Technology Office. All content should be reviewed by the principal or delegate prior to posting any material. Websites that are created without prior approval may be required to remove content or other measures until the approval has been finalized.

Official school and classroom websites and blogs are encouraged to be updated regularly, using the pre-approved building's posting process (Capital School District Acceptable Posting Procedure).

Accessing and updating social media resources for personal use is not permitted during working hours when using personal technology resources, and is not permitted at any time when using Capital School District Resources.

Social media resources may be accessed by specific individuals identified within each school for the purposes of reviewing claims of cyber-bullying, other forms of harassment, and for official purposes preapproved by the district.

The ability to access a resource should not be mistakenly identified as approval, and users run the risk of having those resources blocked in the future. There may also already be established resources that will provide the services being sought. The use of social media resources for instructional purposes must be preapproved by the appropriate district resource prior to usage, and request for approval may be routed through the Technology Office.

Mobile Devices

Capital School District may provide users with mobile computers or other mobile devices to promote learning outside of the classroom, including resources that teachers can use while offsite or at home. Users must adhere to these policies when using Capital School District resources, no matter where or when they are being utilized.

Mobile devices tend to be expensive, and are more susceptible to theft, accidental damage, etc. As such, users are expected to treat these devices with extreme care and caution. Users should report any loss, damage, or malfunction to Technology Office staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse, including theft of equipment entrusted in their care.

School-issued mobile devices may be monitored and controlled, even when off the school's network.

Personal Use of District Resources and Personally-Owned Devices

Users may not use district resources for personal purposes, including the storing of personal images, music, and other data that is not used specifically in classroom instruction. Personal laptops, mobile devices, and other wireless devices should not be connected to the school's network. The introduction of wireless hot spots and other technologies that circumvent filtering is prohibited and will be treated as a severe violation.

While personally owned devices should not be connected to the district's resources as a general rule, some limited use of personal resources may be acceptable. As an example, the use of a personal memory stick would be acceptable if appropriate care has been taken to ensure that the content is free of viruses, malware, etc. The introduction of other technologies must be in compliance with all existing policies, must be approved by a school's principal prior to usage, and must not attach to network resources without the approval of the Technology Office.

Guest Access

In some cases, such as visiting state agencies, consultants, and other individuals visiting in an official Capital School District capacity, access to network resources may be temporarily granted. Prior to access being granted, users should have reviewed the State's and District's Acceptable Use and Internet Safety Policies and should forward the signed acknowledgements to the Technology Office. In an effort to make that process as smooth as possible, advance notice should be provided to the Technology Office. While these devices may not be directly managed by the Technology Office, the Capital School District requires that any connected device receive timely security updates, be protected by current antivirus software, all other standard business protection practices, and may require administrative access to any connected device. The Capital School District also reserves the right to deny access to those unable to comply with this policy.

Wireless

Wireless access is currently restricted to those devices that are directly managed and maintained by the Technology Office. Under no circumstances should access be provided for personal devices, or should any information be released regarding the wireless network. Individuals who are visiting in an official capacity should route their request for access through the Technology Office.

Security

Users are expected to assist in the protection of technology resources and systems. Users who identify a security problem, even those unintentionally created or observed, must notify a system administrator and must not communicate or demonstrate the issue to others. Users should store their passwords securely, should not provide passwords to others, or attempt to log into any system as another user. Violations will result in access and other privileges being revoked. Any user identified as a security risk or having a history of security related issues may also be denied access. Protection of user account logins and passwords is the responsibility of every individual.

The use of strong passwords, as define in the State's Strong Password Authentication Policy (SE-PWD-001) should be used whenever possible. In general, passwords should contain characters from at least three (3) of the following four (4) classes from the table below:

DESCRIPTION	EXAMPLES
English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
English (Arabic) numerals	0, 1, 2, ... 9
English Non-alphanumeric ("special characters")	#,$,%,& such as punctuation symbols etc.

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If you believe a computer or mobile device you are using might be infected with a virus, please alert Technology Office Staff. Do not attempt to remove the virus yourself or download programs advertising the ability to remove viruses.

Privacy, Confidentiality and Public Records Considerations

The Capital School District will make reasonable efforts to maintain the integrity and effective operation of technology systems and resources, but users are advised that those systems should in no way be regarded as a private medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, the district can assure neither the privacy of an individual user's use of district's resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored thereby.

The Capital School District reserves the right to monitor or otherwise intercept any telephone conversation or transmission, electric mail, or Internet access or usage by an employee.

Users should also take every precaution to protect the sensitive data that they interact with. Users should not store sensitive information on personal devices and should report the potential loss of any sensitive data immediately. Providing non-Public information to external or internal resources should not occur without prior approval of appropriate district personal, including the Technology Office. Examples include employee ids, student ids, social security numbers, place of birth, parent's names, and so on. Every system that retains data regarding students, parents, employees, and so on should be reported to the Technology Office. Additional details regarding data classification can be found in the State's Data Classification Policy (IN-DataClass-001).

Limitation of Liability

The Capital School District makes no warranties of any kind, whether expressed or implied, for the services being provided. The Capital School District will not be responsible for any damages to persons, files, data, hardware, or service interruptions. While Capital School District employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. Capital School District will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network. The use of any information obtained via the system is at the user's own risk. Capital School District denies any responsibility for the accuracy or quality of information obtained through the system.

Index of Related Policies

This document should not be viewed as all-inclusive and other policies should be reviewed for additional information. If questions arise regarding any of the policies covered, please contact the Technology Office using the service request processed defined within each school. Below is a list of related policies:

Capital School District:
Acceptable Posting Procedure
Policy #700-31 Bullying Prevention Policy

State of Delaware Policies:
Acceptable Use Policy (DTI-0042.02)
Information Security Policy (SE-ESP-001)
Strong Password Authentication Policy (SE-PWD-001)
Data Classification Policy (IN-DataClass-001)

Additionally, users are encouraged to take the State of Delaware Acceptable Use Policy Self-Test at:
http://dti.delaware.gov/information/aup_self_test.shtml

STAFF APPLICATION FOR ACCESS TO TECHNOLOGY RESOURCES

Below is a list of examples of acceptable and unacceptable uses for your reference. Please understand that the list is not exhaustive and simply serves as a very brief review.

Examples of Acceptable Use — I will…

- ✓ Use school technology systems and resources for academic endeavors.
- ✓ Be respectful of others and encourage responsible online behavior.
- ✓ Use technology resources carefully, and alert staff to any issues with their operation.
- ✓ Recognize that the use of school technologies is a privilege and treat itas such.
- ✓ Proactively help to protect the security of school resources by ensuring that I only open resources known to be secure and by immediately reporting any security related issues.

Examples of Unacceptable Use — I will not…

- ✓ Store personal pictures, movies, and other large files on Capital School District Resources.
- ✓ Try to find ways to circumvent the school's safetymeasures and filtering tools.
- ✓ Use language online that would be unacceptable in the classroom.
- ✓ Attempt to hack or access sites, servers, or content that isn't intended for my use.

I have read and understand the Acceptable Use Policy and agree to abide by it. If I have questions, they will promptly be reported to the Technology Department using the established reporting method. I understand that any violation of these policies could result in loss of access, personal payment of any fees incurred, and possible prosecution. As with other CapitalSchool District policies, any personnel whose conduct violates this policy will be subject to the Capital School District's disciplinary measures, up to andincluding termination.

Date: ______________________ Signature of Applicant: ____

All fields below and on the second page must be completed.

Full Legal Name: ____

Address: ____

____

Birth date: ____________________ **Phone**: ____

School(s)/Building: ____

Position (please check all applicable, or provide details under "Other"):

□ District Office Admin	□ District Office Staff	□ Principal	□ Associate Principal
□ Dean	□ Teacher	□ Special Ed Teacher	□ Instructional Para
□ Extra Support Para	□ Behavior Para	□ Office Para	□ Secretary
□ Clerk	□ Special Ed Coordinator (SEC)	□ BCBA	□ SLP
□ Psychologist	□ Therapist	□ Counselor	□ Instructional Coach
□ Nurse	□ Bus Driver	□ Bus Aide	□ Maintenance
□ Nutritional Staff	□ Custodial	□ SRO / Constable	□ Office of Technology

□ Substitute Teacher or Para	□ Substitute Nurse	□ Substitute Bus Driver
□ Substitute Bus Aide	□ Substitute Secretary	□ Substitute Custodian

Other: ____

Type of Employee:

□ Full Time □ Part Time □ Contractor

Contract Type:

□ 10 month □ 12 month

STUDENT APPLICATION FOR ACCESS TO TECHNOLOGY RESOURCES

Below is a list of examples of acceptable and unacceptable uses for your reference. Please understand that the list is not exhaustive and simply serves as a very brief review.

Examples of Acceptable Use—I will…

- ✓ Use school technology systems and resources for academic endeavors.
- ✓ Be respectful of others and demonstrate responsible online behavior.
- ✓ Alert a teacher or parent if I see threatening, harmful, or offensive materials.
- ✓ Cite sources when using online websites and other resources for research.
- ✓ Recognize that the use of school technologies is a privilege and treat it as such.
- ✓ Protect the safety of myself and others by not disclosing unnecessary personal information.

Examples of Unacceptable Use—I will not…

- ✓ Try to find ways to circumvent the school's safety measures and filtering tools.
- ✓ Attempt to find inappropriate images or content.
- ✓ Engage in cyber-bullying.
- ✓ Agree to meet someone I meet online in real life.
- ✓ Attempt to hack or access sites, servers, or content that isn't intended for my use.

Violations

Violations of this policy may have disciplinary repercussions, including but not limited to the following:

- Suspension of access to technology systems and resources
- Notification of parents or legal guardians
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution

I have read and understand the Acceptable Use Policy, including the consequences of violations listed above, and agree to abide by these policies. If I have questions, they will be discussed with my building administrator(s) and, if required, will be reported to the Technology Office for further review.

Name:____

Address:____

____

Phone:____

School:_________________________ Grade Level(s):________________________

Date: _____________ Signature of Applicant________________________________

If Applicant is under 18 years of age, parent or legal guardian must sign.

Date: _____________ Signature of Parent/Legal Guardian ________________________