Vantage Career Center Technology Plan

Mission Statement: *Vantage provides authentic, student-focused, career technical training that prepares high school students and adults for employment and further education*

Contents

SCHOOL IMPROVEMENT AND TECHNOLOGY PLAN

The Vantage Vocational School Board of Education is committed to the process of continued technology improvement and education and will strive to integrate technology and its components into the daily curricular offering for the students.

The Board will review and approve the district's technology plan.

TECHNOLOGY

The Board of Education is committed to the effective use of technology to both enhance the quality of student learning and the efficiency of District operations.

Students' use of District Technology Resources (see definitions in Bylaw 0100) is a privilege, not a right. Students and their parents must sign and submit a *Student Technology Acceptable Use and Safety* form annually. (See also, Policy 7540.03)

This policy, along with the Student and Staff Technology Acceptable Use and Safety policies, and the Student Code of Conduct, further govern students' and staff members' use of their personal communication devices (see Policy 5136 and Policy 7530.02). Users have no right or expectation of privacy when using District technology resources (including, but not limited to, privacy in the content of their personal files, e-mails and records of their online activity when using the District's computer network and/or Internet connection).

Further safeguards shall be established so that the Board's investment in both hardware and software achieves the benefits of technology and inhibits negative side effects. Accordingly, students shall be educated about appropriate online behavior including, but not limited to, using social media to interact with others online; interacting with other individuals in chat rooms or on blogs; and, recognizing what constitutes cyberbullying, understanding cyberbullying is a violation of Board policy, and learning appropriate responses if they experience cyberbullying.

For purposes of this policy, social media is defined as Internet-based applications that facilitate communication (e.g., interactive/two- way conversation/dialogue) and networking between individuals or groups. Social media is "essentially a category of online media where people are talking, participating, sharing, networking, and bookmarking online. Most social media services encourage discussion, feedback, voting, comments, and sharing of information from all interested parties." [Quote from Ron Jones of Search Engine Watch] Social media provides a way for people to stay "connected or linked to other sites, resources, and people." Examples include Facebook, Twitter, Instagram, webmail, text messaging, chat, blogs, and instant messaging (IM). Social media does not include sending or receiving email through the use of District-issued email accounts.

The Board prohibits students from using District Technology Resources to access and/or use social media.

Staff may use social media for business-related purposes. Authorized staff may use District Technology Resources to access and use social media to increase awareness of District programs and activities, as well as to promote achievements of staff and students, provided the Superintendent approves, in advance, such access and use. Use of social media for business-related purposes is subject to Ohio's public records laws and staff members are responsible for archiving their social media and complying with the District's record retention schedule. See Policy 8310 – Public Records and AG 8310A - Public Records.

Staff must comply with Policy 7540.04 and Policy 7530.02 when using District Technology Resources to access and/or use social media.

COMPUTER TECHNOLOGY AND NETWORKS

The Technology Supervisor is responsible for managing the Board of Education's technology system and making arrangements for any networks that may be used to enhance the educational program and/or operations of the District.

S/He also is responsible for implementing the guidelines established for program development (AG 2210A through AG 2252), the selection of materials and equipment (AG 2520A), and verifying that the District's purchasing guidelines (AG 6320A) are followed. In addition, the Technology Supervisor shall verify that each staff member and student who will have access to Board technology and any networks completes the appropriate agreement Form 7540.04 F1 or Form 7540.03 F1.

All tentative agreements with networks or technology agencies are to be submitted to the Superintendent for review and approval.

Staff members and/or students are to be provided the following information concerning the use of the Internet:

A. Use of the Internet is to be related to one or more courses of study and is not to be used by staff or students for discriminatory or unlawful purposes. Further, use of the Internet for recreational or personal purposes is prohibited. All student use is to be supervised by a staff member or approved volunteer who has signed the Staff Network and Internet Acceptable Use and Safety Agreement Form 7540.04 F1.

B. Prior to disseminating information across the Internet about a student such as name, address, or other identifying data including pictures, signed parental permission forms must be on file.

C. Because of the vast amount of information that can be retrieved from the Internet teachers are responsible for training students to use proper research skills when retrieving information. It is inappropriate, costly, and a waste of valuable instructional time for staff and/or students to download large quantities of information that has not been checked ahead of time for accuracy, relevancy, and probable usage. It may be helpful, therefore, for teachers to conduct some controlled exercises with students on how to differentiate between websites that are "attractive but superficial or irrelevant" from those that are "attractive, substantive, and relevant."

D. Staff members need to have back-up plans or contingency procedures in place for times when the Internet may not be accessible. Since the Internet is primarily a data-gathering mechanism,

alternative sources for needed data should be available so that students can accomplish the purpose of the instruction within the established time period.

E. The Student and Staff Network and Internet Acceptable Use and Safety Agreements, Form 7540.03 F1 and Form 7540.04 F1, that students and staff members must sign prohibits the use of the Internet for illegal, unethical, or harassing purposes or to obtain information that could be considered obscene, pornographic, or unsuitable for children. If a question of interpretation arises concerning the definition of these terms, the Superintendent and building director shall have the authority to determine whether the website is appropriate or the use is permissible. Prior to accessing or allowing access to information that the staff member is unsure about, s/he should consult with the Technology Supervisor.

F. As students and/or staff members complete projects that reflect unusual and creative applications of technology, the projects should be shared with the supervisor so that proper publicity can be created as appropriate to the project. It is essential that the Student and Staff Network and Internet Acceptable Use and Safety Agreements, Form 7540.03 F1 and Form 7540.04 F1, address the issue of the proprietary rights related to website design concerning websites and/or pages hosted on the Board's servers and/or created during work time as part of an employee's job responsibilities (staff) or as a class assignment (students).

This information can be provided through written guidelines, professional development seminars, faculty and student meetings, and introductory remarks at the beginning of a course in which the Internet may be used.

SECURITY PROCEDURES FOR TECHNOLOGY RESOURCES (AS DEFINED IN BYLAW 0100)

A. Identification:

1. Each District Technology Resource shall have a label that states the District's name and an identification number.

2. The Treasurer shall maintain a record of the identification number, serial number, model, etc. for each District Technology Resource.

3. The Technology Supervisor shall maintain up-to-date software licenses and related records concerning software/applications used in the District, including the course or program in which it is used.

B. Use of District Technology Resources:

District Technology Resources, regardless of whether they will be used on District property or off-school premises, must be checked out through the technology Supervisor. (See Form 7530A F1.) District Technology Resources shall not be used for the purpose of copying materials in violation of copyright laws or in a manner inconsistent with applicable policies and guidelines that address its use. See Policy 7530.01, Policy 7540.01, Policy 7540.02, Policy 7540.04, and AG 2531, AG 7540, AG 7540.01A, AG 7540.01B, AG 7540.02, AG 7540.04, and AG 7540.05.)

The person signing the request Form 7530A F1 is responsible for the condition of the District

Technology Resource until it is checked back in.

Students are not to use District Technology Resources without first receiving appropriate training.

In special circumstances, students may be allowed to use District Technology Resources, without supervision, when the teacher in charge deems it appropriate and the student has proved himself/herself responsible.

Where an exceptional instructional need is demonstrated, permission to use District Technology Resources off school premises shall be granted by the director after consulting technology Supervisor. (Use Form 7530A F1.)

Exceptional instructional needs include, but are not limited to:

1. increasing teacher proficiency in the operation of equipment or enlarging knowledge of particular software/application necessary for classroom instruction;

2. producing/preparing instructional materials or classroom lessons;

3. developing new or additional applications of District Technology Resources;

4. allowing students to do homework assignments or self-tutoring.

C. Requests for Personal Use:

Personal use of District Technology Resources, including computers and peripherals, by students, staff, and District residents shall be in accordance with Policy 7530 and the accompanying guidelines.

Requests to use District Technology Resources for personal use off school premises will require written permission from technology Supervisor.

D. Staff Services:

IT staff will instruct the user on the correct operation of District Technology Resources prior to the user receiving the item/equipment. The Technology Supervisor will designate appropriate staff to assist in moving and setting up District Technology Resources for instructional purposes on school premises.

IT staff may assist other staff members in obtaining materials for instructional use by video or audio recording within copyright guidelines.

E. Inventory and Repair of District Technology Resources:

All District Technology Resources will be inventoried at the end of each school year. Technology Supervisor shall maintain an accurate inventory of all District Technology Resources. Inventory will also be maintained in the school or department in which they are located.

If a District Technology Resource requires repair, it will be sent to the Technology Supervisor

F. Report of Loss:

If any District Technology Resource is lost, the director and the Superintendent shall be notified. The Superintendent should notify police, if deemed appropriate. A complete inventory of all other District Technology Resources located in the same area as the lost items shall be taken. Inventory records for all missing equipment/software shall be kept in a separate file for use in giving information to the police and/or the insurance company.

ELECTRONIC DATA DISASTER RECOVERY PLAN

The Vantage Career Center recognizes the importance of maintaining the strategies, personnel, procedures, and resources necessary to respond to any short or long term emergencies that might interrupt the Information Technology (IT) functions of the District. This Electronic Data Disaster Recovery Plan outlines operational procedures intended to prevent data loss, minimize loss of access, and provide response strategies for both Level I and Level II emergencies.

The Superintendent shall activate the Recovery Team upon discovery of any incident that has the potential for significantly interrupting computer service and/or the IT functions of the District.

Operational Procedures

The Technology Supervisor shall implement the following procedures and safeguards of the District's electronic network and systems:

A. Provide for a minimum of a 4-month retention period on all data.

B. Provide for the full back up of each server every 2 weeks. This back up shall be stored at an alternate site in a fireproof safe. The location of the alternate site shall be determined by NOACSC, with the location and access information filed with the Superintendent and the Treasurer.

C. Run incremental back up on each server nightly between full back operations. This back up shall be stored in a fireproof safe at the A site

D. Provide for secure backup of the District's payroll. Note: District payroll is maintained on a separate State supported software which is cloud based. Backup and support for this software is managed through the A site

E. Provide for backup of the student server daily, with storage of data in a fireproof safe located in NOACSC.

System Information

The Technology Supervisor shall maintain the following information:

A. A reciprocal agreement with NOACSC, outlining the scope of reciprocal services, location and access to the alternative facility, computer time, personnel assistance, and costs.

B. Specifications for all District data equipment.

C. District insurance information, including contact information and limits of coverage and liability.

D. A list of applications and software used by the District, along with their corresponding licenses and/or proof of purchases and warranty information.

E. Documentation of procedures used to back up all programs and data.

F. Location and access of all back up data, both in-district and off-site.

G. Maintenance agreements for hardware and software.

H. A list of vendor contacts capable of assisting in the immediate replacement of disabled equipment or corrupted software.

Level I Emergency Procedures

Level I Emergencies typically include such minor occurrences as short term power outages and incidental loss of data. In such situations, The Technology Supervisor shall notify the Superintendent of the interruption to computer service and advise of the strategies being utilized to restore service and data to affected users. The deployment of back-up generator power, the use of uninterruptible power supply (UPS), and access of back up data (redundancy protection) shall be reported to the Superintendent, along with cost assessment of restoring service and data.

Level II Emergency Procedures

Level II Emergencies include occurrences of a greater magnitude such as long term power outages, natural disaster, fire damage, theft, vandalism, criminal damaging, or major equipment malfunction. In such situations, The Technology Supervisor shall notify the Superintendent of the interruption to computer service immediately. The Superintendent will activate the Recovery Team necessary to implement response strategies based on the particular incident.

The Superintendent shall make critical determinations regarding damage assessment, plan implementation, support services deployed, and acquisition and utilization of resources.

The Recovery Team shall assist the Superintendent with unique knowledge and technical skills regarding IT functions and response and recovery activities. The Technology Supervisor shall direct the Recovery Team and implement the recovery plan. Duties shall include, but not be limited to:

A. require that all appropriate emergency response procedures are followed;

B. establish communications with the Recovery Team and maintain ongoing communications with the Superintendent;

C. determine location for initial reporting of Recovery Team and alert location staff of arrival;

D. gather and organize information about the incident and corresponding response and recovery requirements;

E. maintain and disseminate Incident Status Summary reports;

F. assist the Recovery Team in developing and implementing response and recovery strategies.

The Recovery Team shall implement the recovery plan, as directed. Duties shall include, but not be limited to:

A. participate in Incident Management Plan activities;

B. inform and assign personnel in accordance with the recovery strategies;

C. supervise/implement operations at the designated recovery site;

D. report progress and problems to The Technology Supervisor and the Superintendent.

TECHNOLOGY PRIVACY

The Board of Education recognizes its staff members' right to privacy in their personal lives. This policy serves to inform staff members of the Board's position with respect to staff-member privacy in the educational and workplace setting and to protect the Board's interests.

All District Technology Resources (as defined in Bylaw 0100) are the Board's property and are intended to be used for business purposes. The Board retains the right to access and review all Information Resources (as defined in Bylaw 0100), including but not limited to electronic and voice mail, computer files, databases, and any other electronic transmissions contained in or used in conjunction with the Board's computer system/network, telephone system, electronic mail system, and voice mail system. Staff members shall be notified that they have no expectation that any personal information/data maintained, stored, or transmitted on or through such systems is confidential or private.

Review of such information may be done by the Board with or without the staff member's knowledge. The use of passwords does not guarantee confidentiality, and the Board retains the right to access information in spite of a password. All passwords or security codes must be registered with the Board. A staff member's refusal to permit such access may be grounds for discipline up to and including discharge.

District Technology Resources are to be used only for business and educational purposes.

Personal messages via Board-owned technology should be limited in accordance with the Superintendent's guidelines. Staff members are encouraged to keep their personal records and personal business at home. Because District Technology Resources are to be used primarily for business and educational purposes, staff members are prohibited from sending offensive, discriminatory, or harassing computer, electronic, or voice mail messages.

District Technology Resources must be used properly. Review of computer files, electronic mail, and voice mail will only be done in the ordinary course of business and will be motivated by a legitimate business reason. If a staff member's personal information is discovered, the contents of such discovery will not be reviewed by the Board, except to the extent necessary to determine if the files/e- mail/voice mail constitute a public record or if the Board's interests have been compromised. Any information discovered will be limited to those who have a specific need to know that information.

The administrators and supervisory staff members authorized by the Superintendent have the authority to search and access information electronically.

All District Technology Resources and District Information Resources are the property of the Board. Staff members shall not copy, delete, or remove any information/data contained on District Technology Resources without the express permission of the Superintendent, or communicate any such information to unauthorized individuals. In addition, staff members may not copy software onto any District Technology Resources and may not bring software from outside sources for use on District Technology Resources without the prior approval of the Technology Supervisor. Such pre-approval shall include a review of any copyright infringements or virus problems associated with such outside software.

STAFF EDUCATION TECHNOLOGY ACCEPTABLE USE AND SAFETY

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 Education provides Technology and Information Resources (as defined by Bylaw 0100) to support the educational and professional needs of its staff and students. The Board provides staff with access to the Internet for limited educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students and to facilitate the staff's work. The District'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.

The Board regulates the use of District Technology and Information Resources by principles consistent with applicable local, State, and Federal laws, and the District's educational mission. This policy and its related administrative guidelines and any applicable employment contracts and collective bargaining agreements govern the staffs' use of the District's Technology and Information Resources and staff's personal communication devices when they are connected to the District's computer network, Internet connection and/or online educational services/apps, or when used while the staff member is on Board-owned property or at a Board-sponsored activity (see Policy 7530.02).

Users are required to refrain from actions that are illegal (such as libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, and the like) or unkind (such as personal attacks, invasion of privacy, injurious comment, and the like). Because its Technology Resources are not unlimited, the Board has also instituted restrictions aimed at preserving these resources, such as placing limits on use of bandwidth, storage space, and printers.

Users have no right or expectation to privacy when using District Technology and Information Resources (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity when using the District's computer network and/or Internet connection).

Staff members are expected to utilize District Technology and Information Resources 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 Board Policy 2520 - Selection of Instructional Materials and Equipment.

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 District 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, District Technology Resources provide 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, the Board may not be able to technologically limit access, through its Technology Resources, 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 guidelines 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 that 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 Superintendent, the technology protection measures may also be configured to protect against access to other material considered inappropriate for students to access. The Board also 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. The technology protection measures, may not be disabled at any time that students may be using the District Technology Resources, 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 without express written consent of an appropriate administrator will be subject to disciplinary action, up to and including termination.

In order to follow CIPA regulations (Child Internet Protection Act), staff are prohibited from creating hotspots with personal electronic communication devices including all phones. Doing so bypasses any security measures created by the district to comply with CIPA.

The Superintendent or Technology Supervisor may temporarily or permanently unblock access to websites or online educational services/apps 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 Superintendent or Technology Supervisor may also disable the technology protection measures to enable access for bona fide research or other lawful purposes.

Staff members will participate in 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", "harvesting", "digital piracy", "data mining", etc., cyberbullying and other unlawful or inappropriate activities by students or staff online; and

D. unauthorized disclosure, use, and dissemination of personally-identifiable information regarding minors.

Furthermore, staff members shall provide instruction for their students regarding the appropriate use of technology and online safety and security as specified above, and staff members will monitor students' online activities while 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.

Building Directors are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying guidelines. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of the District Technology Resources. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social media including in chat rooms and cyberbullying awareness and response. All users of District Technology Resources are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines.

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

With prior approval from the Superintendent or Technology Supervisor, staff may direct students who have been issued school-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.

Staff members are responsible for good behavior when using District Technology and Information Resources - i.e., behavior comparable to that expected when as they are in classrooms, school hallways, and other school premises and school sponsored events. Communications on the Internet are often public in nature. The Board does not approve any use of its Technology and Information Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

Staff members may only use District Technology Resources to access or use social media if it is done for educational or business-related purposes.

General school rules for behavior and communication apply.

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users are personally responsible and liable, both civilly and criminally, for uses of District Technology and Information Resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the Superintendent and Director as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to staff members' use of District Technology and Information Resources.

Social Media Use

An employee's personal or private use of social media may have unintended consequences. While the Board respects its employees' First Amendment rights, those rights do not include permission to post inflammatory comments that could compromise the District's mission, undermine staff relationships, or cause a substantial disruption to the school environment. This warning includes staff members' online conduct that occurs off school property including from the employee's 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 their 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. Staff members who violate State and Federal confidentiality laws or privacy laws related to the disclosure of confidential student or employee information may be disciplined.

Staff members retain rights of communication for collective bargaining purposes and union organizational activities.

Student Acceptable Use

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 Education provides Technology Resources (as defined in Bylaw 0100) to support the educational and professional needs of its students and staff. With respect to students, District Technology Resources afford them the opportunity to acquire the skills and knowledge to learn effectively and live productively in a digital world. The Board provides students with access to the Internet for limited educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students. The District's computer network and 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.

The Board regulates the use of District Technology Resources by principles consistent with applicable local, State, and Federal laws, the District's educational mission, and articulated expectations of student conduct as delineated in the Student Code of Conduct. This policy and its related administrative guidelines and the Student Code of Conduct govern students' use of District Technology Resources and students' personal communication devices when they are connected to the District computer network, Internet connection, and/or online educational services/apps, or when used while the student is on Board-owned property or at a Board-sponsored activity see Policy 5136).

Users are required to refrain from actions that are illegal (such as libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, and the like) or unkind (such as personal attacks, invasion of privacy, injurious comment, and the like). Because its Technology Resources are not unlimited, the Board has also instituted restrictions aimed at preserving these resources, such as placing limits on use of bandwidth, storage space, and printers.

Users have no right or expectation to privacy when using District Technology Resources (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity when using the District's computer network and/or Internet connection). First, the Board may not be able to technologically limit access, through its Technology Resources, 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 guidelines 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, that 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 Superintendent, the technology protection measures may be configured to protect against access to other material considered inappropriate for students to access. The Board 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. The technology protection measures may not be disabled at any time that students may be using District Technology Resources, 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.

In order to follow CIPA regulations (Child Internet Protection Act), staff are prohibited from creating hotspots with personal electronic communication devices including all phones. Doing so bypasses any security measures created by the district to comply with CIPA.

The Superintendent or Technology Supervisor may temporarily or permanently unblock access to websites or online educational services/apps 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 are advised that a determined user may be able to gain access to services and/or resources 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 may find inappropriate, offensive, objectionable or controversial. Parents of minors are responsible for setting and conveying the standards that their children should follow when using the Internet.

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", "harvesting", "digital piracy", "data mining", etc.), cyberbullying and other unlawful or inappropriate activities by students online, and

D. unauthorized disclosure, use, and dissemination of personally-identifiable information regarding minors

Staff members shall provide instruction for their students regarding the appropriate use of technology and online safety and security as specified above. Furthermore, staff members will monitor the online activities of students while 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.

Building Directors are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying guidelines. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of District Technology

Resources. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social media including in chat rooms and cyberbullying awareness and response. All users of District Technology Resources (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 guidelines.

Students will be assigned a school email account that they are required to utilize for all school-related electronic communications, including those to staff members, peers, and individuals and/or organizations outside the District with whom they are communicating for school-related projects and assignments. Further, as directed and authorized by their teachers, they shall use their school-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 are responsible for good behavior when using District Technology Resources – i.e., behavior comparable to that expected of students when 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 approve any use of its Technology Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

Students may only use District Technology Resources to access or use social media if it is done for educational purposes in accordance with their teacher's approved plan for such use.

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users are personally responsible and liable, both civilly and criminally, for uses of District Technology Resources that are not authorized by this Board policy and its accompanying guidelines.

The Board designates the Superintendent and Technology Supervisor as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to students' use of District Technology Resources.

As set forth in Policy 7540.03 – Student Technology Acceptable Use and Safety and Policy 7540.04 – Staff Technology Acceptable Use and Safety, the District will provide students and staff members with the training required by Federal and State law.

In addition, staff members and/or students shall be provided the following information/training concerning the use of the Internet:

A. Use of the Internet is to be related to one (1) or more courses of study and is not to be used by staff or students for discriminatory or unlawful purposes. All student use is to be supervised by a staff member or approved volunteer who has signed the Staff Technology Acceptable Use and Safety Agreement Form 7540.04 F1.

B. Because of the vast amount of information that can be retrieved from the Internet, teachers are responsible for training students to use proper research skills when retrieving information. It is inappropriate, costly, and a waste of valuable instructional time for staff and/or students to download large quantities of information that has not been checked ahead of time for accuracy,

relevancy, and probable usage. It may be helpful, therefore, for teachers to conduct some controlled exercises with students on how to differentiate between websites that are "attractive but superficial or irrelevant" from those that are "attractive, substantive, and relevant."

C. Staff members need to have back-up plans or contingency procedures in place for times when the Internet may not be accessible. Since the Internet is primarily a data-gathering mechanism, alternative sources for needed data should be available so that students can accomplish the purpose of the instruction within the established class period.

D. The Student and Staff Technology Acceptable Use and Safety Agreements, Form 7540.03 F1 and Form 7540.04 F1, prohibit the use of the Internet for illegal, unethical, or harassing purposes or to obtain information that could be considered obscene, pornographic, or unsuitable for children. If a question of interpretation arises concerning the definition of these terms, the Superintendent shall have the authority to determine whether the website is appropriate or the use is permissible. Prior to accessing or allowing access to information that the staff member is unsure about, s/he should consult with Technology Supervisor.

E. As students and/or staff members complete projects that reflect unusual and creative applications of technology, the projects should be shared with the High School Director so that proper publicity can be created as appropriate to the project. It is essential that the Student and Staff Technology Acceptable Use and Safety Agreements, Form 7540.03 F1 and Form 7540.04 F1, address the issue of the proprietary rights related to the design and development of web pages, sites, services or apps hosted on Board-owned or District-affiliated servers that are created during work time as part of an employee's job responsibilities (staff) or as a class assignment (students).

This information can be provided through written guidelines, professional development seminars, faculty and student meetings, and introductory remarks at the beginning of a course.

PERSONAL USE OF DISTRICT TECHNOLOGY RESOURCES

The following guidelines govern staff member's personal use of District Technology Resources (as defined in Bylaw 0100) either at school or while at home for school purposes. These guidelines also govern students' personal use of District Technology Resources while at home. Except as authorized herein, no personal, that is, non-school, use of District Technology Resources may be made by any student at any time.

A. Any software that is installed on any district resource is acquired and approved through the Technology request process. These requests are reviewed, and approved by the administrative team for purchase from the Technology budget.

B. A staff member or a student may start a project using Board-owned software or personal software and produce a copy of the project or document. Ordinarily, the Board will not provide Board-owned software for use on a personal communication devices (PCD) (as defined in Bylaw

0000) owned by a staff member or student. When the project is completed, the staff member or student should notify the Technology Supervisor to find out whether or not the Board wants to keep a copy for reference or for use by others. No staff member or student should expect to retain any proprietary rights related to the design or content of any web sites, pages, services or apps hosted on Board-owned or District-affiliated servers or that are created during work as a part of an employee's job responsibilities (staff) or as a class assignment (student).

C. Prior to making a copy of or using any Board-owned software, a staff member or student should contact the Technology Supervisor to find out whether or not there is any licensing agreement associated with that software, and if so, whether the license allows the staff member or student to load the material on or access the product/services through his/her personal computer. If reproduction is allowed, the staff member or student is to complete a check-out form (see Form 7540.01 F2) in which s/he agrees to make only one copy and only for personal use and not for use by others. If the license does not allow this, then no copy is to be made.

D. Before accessing District Technology Resources, including the Internet or District network(s), staff members and students must sign the applicable Student or Staff Technology Acceptable Use and Safety Agreement, Form 7540.03 F1 or Form 7540.04 F1. All student use of the Internet must be under the supervision of a staff member or approved volunteer.

E. Neither staff members nor students are to use District Technology Resources for recreational, personal, discriminatory, or unlawful purposes but only for purposes related to the Board's educational mission and goals, program or operational needs.

F. Each staff member and student will be issued a password for use with District Technology, provided the individual agrees not to share the password with others. The existence of a password does not guarantee confidentiality or privacy and the Board retains the right to use any person's password to monitor the type of use that is being made of the District Technology Resource.

G. With regard to personal email, staff members may use it to send and/or receive personal messages provided such use their District-issued e-mail account to send and/or receive personal messages is limited to non-duty time and does not involve the conduct of any personal, discriminatory, or unlawful business (including commercial purposes, advertising, and political lobbying).

H. Students are not allowed to send or receive personal e-mail messages using District Technology Resources.

I. Use of all other District Technology Resources shall be in accord with AG 7530A - Personal Use of

ACCESS TO DISTRICT TECHNOLOGY RESOURCES AND/OR INFORMATION RESOURCES FROM PERSONAL COMMUNICATION DEVICES

For purposes of this policy, “personal communication device” (PCD) includes computers, tablets (e.g., iPad-like devices), electronic readers (“e-readers”; e.g., Kindle-like devices), cell phones, smartphones

(e.g., iPhones, Android devices, Windows Mobile devices, etc.), telephone paging devices (e.g., beepers or pagers), and/or other web-enabled devices of any type.

The Board of Education provides both a guest network and business network. The business network is a secure network for the conduct of official District business. Access to the business network requires prior approval and authorization by the District. The guest network is a CIPA-compliant non-secured network provided for use by students, parents, and other visitors while on school property. Only Board-approved communication devices and authorized users may access the business network. Any non-Board-approved communication devices or non-authorized users must be pre-approved by the Superintendent.

The Board of Education prohibits individuals from using their PCDs to access District Technology Resources (as defined in Bylaw 0100) while on-site at a District facility.

Exceptions to this policy must be approved in advance, in writing, by the Technology Supervisor or Superintendent.

The Board provides staff members, students, and members of the community with access to the Board's network and/or the Internet through the use of their home computers in accordance with the following guidelines:

A. The amount of access time the Board will allow is unlimited.

B. The Board will not provide help-desk support.

C. The Board will provide log-on instructions for IBM compatible PC's.

D. The Board will not be responsible for:

    1. any content that a home-user may access through the Internet;

    2. any virus that a home-user may obtain while accessing the Internet through Board technology;

    3. any copyright violations that may be incurred while accessing the Internet through Board technology;

    4. loss of or damage to any equipment of the home-user.

E. The Board will not allow a home-user to establish personal e-mail accounts through Board technology.

F. All information sent, received, or transmitted using Board technology or stored on Board servers, including, but not limited to, e-mail, shall be considered Board property and there shall be no expectation of privacy or confidentiality concerning same. The Board reserves the right to access such information at any time.

G. The Technology Supervisor is responsible for creating a Network and Internet Acceptable Use and Safety Agreement Form which clearly states that when a person uses Board technology to create a web site or page which is hosted on Board servers, s/he acknowledges that the Board is entitled to any and all proprietary rights related to said web site and/or pages.