COMPUTER TECHNOLOGY AND NETWORKS

The Board is committed to the effective use of technology to both enhance the quality of student learning and the efficiency of operations within the school system.

However, the use of the Academy's network and technology resources by students is a privilege, not a right. As a prerequisite, students and their parents must sign and submit a *Student Network and Internet Acceptable Use and Safety* form ( ) annually. (See also, Policy 7540.03)

The ESP shall develop and ***P 7540 STP Plan*** a written School Technology Plan (STP). Procedures for the proper acquisition of technology shall be set forth in the STP. The STP shall also provide guidance to staff and students about making safe, appropriate and ethical use of the Academy's network(s), as well as inform both staff and students about disciplinary actions that will be taken if Board technology and/or networks are abused in any way or used in an inappropriate, illegal, or unethical manner.

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 Academy policy, and learning appropriate responses if they are victims of cyberbullying.

The Board authorizes the access and use of social media from the Academy's network to increase awareness of Academy programs and activities, as well as to promote achievements of staff and students, provided such access and use is approved in advance by the School Leader.

The ESP shall review the STP and ***P 7540 STP Update Options*** any changes, amendments or revisions to the Board annually.

TECHNOLOGY PRIVACY

The Board recognizes the right to privacy of staff members in their personal lives. This policy serves to inform staff members of the Board's position regarding staff members' privacy in the educational workplace setting. The policy also serves to protect the Board's interests.

All computers, telephone systems, electronic mail (e-mail) systems, and voice mail systems are the Board's property and are to be used solely for business purposes. The Board retains the right to access and review all electronic and voice mail, computer files, data bases, and any other electronic transmissions contained within, or used in conjunction with, the Board's computer system, telephone system, electronic mail system, and voice mail system. Staff members should not expect any information contained on such systems to be 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.

Computers, electronic mail, and voice mail are to be used only for the Academy's business and educational purposes.

Personal messages via Board-owned technology should be limited, in accordance with the ESP Administrative Procedures.

Staff members are prohibited from sending offensive, discriminatory, or harassing messages via Board-owned technology: computer, electronic mail, or voice mail.

The Board requires the proper use of its resources. Review of computer files, electronic mail, and voice mail will be conducted only 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 be limited to those who have a specific need to know that information. The discovered contents will not be reviewed by the Board, except to the extent necessary to determine if the Board's interests have been compromised. The administrators and supervisory staff members authorized by the ESP have the authority to search and access information electronically.

All computers and any information or software contained therein are property of the Board. Staff members shall not copy, delete, or remove any information or data contained on the Board-owned computers or servers without the express permission of the School Leader or designee. Further, staff members shall not communicate any such information to unauthorized individuals. In addition, staff members may not copy software from or onto any Board computer and may not bring software from outside sources for use on Board equipment without the prior approval of the ESP. Such pre-approval will include a review of any copyright infringements or virus problems associated with such outside software.

ACADEMY WEB PAGE

The Board authorizes the creation of Web sites by staff and students of the Academy to be published on the Internet. The creation of Web sites by students must be done under the supervision of a professional staff member. These Web sites must reflect the professional image of the Academy, its personnel, and students. The content of all pages shall be consistent with the Board's Mission Statement and subject to prior approval of the ESP.

The purpose of such Web sites is to educate, inform, and communicate. The following criteria should be used to guide the development of Web sites:

A. Content should be suitable and usable for students and teachers to support the curriculum and the Board's educational goals and objectives as listed in the Board's Strategic Plan.

B. Content should inform the community about the Academy, teachers, students, or departments, including information about curriculum, events, class projects, student activities, and departmental policies.

C. Content should provide an avenue to communicate with the community.

The information contained on the Web site should reflect and support the Board's Mission Statement, Educational Philosophy, and the School Improvement Process.

When the content includes a photograph or information relating to a student, the Board will abide by the provisions of Policy 8330 - Student Records.

All links included on the pages must also meet the above criteria and comply with State and Federal laws (e.g., copyright laws, Children's Internet Protection Act), ADA, Children's Online privacy Protection Act (COPPA)). Nothing in this paragraph shall prevent the Academy from linking the Board's website to (1) recognized news/media outlets (e.g., local newspapers' websites, local television stations' websites) or (2) to websites that are developed and hosted by outside commercial vendors pursuant to a contract with the Board. The Board recognizes that such third party websites may contain age appropriate advertisements that are inconsistent with the requirements of Policy 9700.01, AG 9700B, and State and federal Law.

Under no circumstances is a Web site to be used for commercial purposes advertising, political lobbying, or providing financial gains for any individual. ncluded in this prohibition is the fact no webpages contained on the Academy's website may: (1) include statements or other items that support or oppose a candidate for public office or a ballot proposal, the investigation, prosecution or recall of a public official, or passage of a tax levy or bond issue; (2) link to a website of another organization if the other website includes such a message; (3) communicate information that supports or opposes any labor organization or any action by, on behalf of, or against any labor organization; or communicate a political position or advocate for an issue.

Under no circumstances is a staff member-created webpage/site including personal webpages/sites, to be used to post student progress reports, grades, class assignments, or any other similar class-related material. The board maintains its own website (e.g., [Progressbook]) that employees are required to use for the purpose of conveying information to students and/or parents.

Staff members are prohibited from requiring students to go to the staff member's personal webpages/sites (including, but not limited to, their Facebook or MySpace pages) to check grades, obtain class assignments and/or class-related materials, and/or to turn in assignments.

If a staff member creates a webpage/site related to his/her class, it must be hosted on the Board's server.

Unless the webpage/site contains student personally identifiable information, Board websites that are created by students and/or staff members that are posted on the Internet should not be password protected or otherwise contain restricted access features, whereby only employees, student(s), or other limited groups of people can access the site. Community members, parents, employees, staff, students, and other website users will generally be given full access to the sites created pursuant to this policy.

Such Web sites should address both internal and external audiences who will view the information. Academy Web sites must be located on Board-affiliated servers.

The Board retains all proprietary rights related to the design of Web sites and/or pages hosted on the Board's servers, absent written agreement to the contrary.

Students who want their class work to be displayed on the Board's Web site must have written parental permission and must expressly license the display without cost to the Board. Prior written parental permission is necessary for a student to be identified by name anywhere on the Board's Web site.

The ESP shall prepare Administrative Guidelines defining the standards permissible for Web site use.

STUDENT EDUCATION ACCEPTABLE USE AND SAFETY

Reference: 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 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).

First, and foremost, the Board may not be able to technologically limit access to services through 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, will open 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, or designee. The ESP or School Leader, or designee 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 ESP 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 ESP to implement procedures regarding the appropriate use of technology and online safety and security as specified above. Furthermore, the ESP 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 ESP 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 and staff members are responsible for good behavior on the Academy'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.

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 ESP and Technology Coordinator 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.

STAFF NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY

Reference: 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 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 an 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 Education Technology, students and staff can access relevant information that will enhance their learning and the education process. Further, the Internet 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, will open classrooms and students to electronic information resources that not have been 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 ESP, 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, or designee.

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 ESP or Technology Coordinator 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 ESP 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 ESP 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 ESP to cause to provide instruction for students regarding the appropriate use of technology and online safety and security as specified above, and the ESP 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.
The ESP 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 Internet. 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.

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 Academy'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 Academy's Mission, undermine staff relationships, or cause a substantial disruption to the school environment. This warning includes Academy personnel online conduct that occurs off school property, including from the Academy'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 Academy 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. Academy 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 ESP and Technology Coordinator 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.

ELECTRONIC MAIL

The Board is committed to the effective use of electronic mail ("e-mail") by all school staff and Board members in the conduct of their official duties. This policy, as well as any procedures developed pursuant to it, are not meant to limit or discourage the use of e-mail for conducting the official business of the Academy, but rather, this policy and any corresponding procedures are intended to establish a framework for the proper use of e-mail as an official business tool.

When available, the Academy's e-mail system must be used by ESP for any official Academy e-mail communications. Personal e-mail accounts on providers other than the Academy's e-mail system may be blocked at any time due to concerns for network security, SPAM, or virus protection. Furthermore, school staff are expected to exercise reasonable judgment and prudence and take appropriate precautions to prevent viruses from entering the Academy's network when opening or forwarding any e-mails or attachments to e-mails that originate from unknown sources.

School staff shall not send or forward mass e-mails, even if the e-mails concern Academy business, without prior approval of the Educational Service Provider.

School staff may join list servs or other e-mail services (e.g. RSS feeds) that pertain to their responsibilities in the Academy, provided these list servs or other e mail services do not exceed the staff member's e-mail storage allotment. Staff members are required to keep their inbox and folders organized by regularly reviewing e-mail messages, appropriately saving e-mails that constitute a public record or student record and e-mails that are subject to a Litigation Hold, and purging all other e mails that have been read. If the staff member is concerned that his/her e-mail storage allotment is not sufficient, s/he should contact the Academy's technology coordinator (IT staff). Similarly, if a staff member is unsure whether s/he has adequate storage or should subscribe to a list serv or RSS feed, s/he should discuss the issue with his/her School Leader or the Academy's technology coordinator. The Educational Service Provider is authorized to block e-mail from list servs or e-mail services if the e-mails received by the staff member(s) regularly exceed 50 megabytes.

Public Records

The Academy complies with all Federal and State laws pertaining to electronic mail. Accordingly, e-mails written by or sent to school staff and Board members may be public records if their content concerns Academy business, or education records if their content includes personally identifiable information about a student. E-mails that are public records are subject to retention and disclosure, upon request, in accordance with Policy 8310 – Public Records. E-mails that are student records should be maintained pursuant to Policy 8330 – Student Records. Finally e-mails may constitute electronically stored information ("ESI") that may be subject to a Litigation Hold pursuant to Policy 8315 – Information Management.

State and Federal law exempt certain documents and information within documents from disclosure, no matter what their form. Therefore, certain e-mails may be exempt from disclosure or it may be necessary to redact certain content in the e mails before the e–mails are released pursuant to a public records request, the request of a parent or eligible student to review education records, or a duly served discovery request involving ESI.

E-mails written by or sent to school staff and Board members by means of their private e-mail account may be public records if the content of the e-mails concerns Academy business, or

education records if their content includes personally identifiable information about a student. Consequently, staff shall comply with an Academy request to produce copies of e-mail in their possession that are either public records or education records, or that constitute ESI that is subject to a Litigation Hold, even if such records reside on a computer owned by an individual staff member, or are accessed through an e-mail account not controlled by the Academy.

Retention

Pursuant to State and Federal law, e-mails that are public records or education records, and e-mails that are subject to a Litigation Hold shall be retained.

E-mail retention is the responsibility of the individual e-mail user. E-mails sent or received using the Academy's e-mail service may only be retained for 30 days on the server. This retention is for disaster recovery and not to provide for future retrieval. The Academy does not maintain a central or distributed e-mail archive of e mail sent and/or received.

The Academy maintains archives of all e-mails sent and/or received by users of the Academy's e-mail service. Staff members are required to forward copies of any e-mails received in their personal e-mail account(s) not affiliated with the Academy server to their Academy e-mail account so that these records are also archived for future retrieval, if necessary.

Unauthorized E-mail

The Board does not authorize the use of its proprietary computers and computer network ("network") to accept, transmit, or distribute unsolicited bulk e-mail sent through the Internet to network e-mail accounts. In addition, Internet e-mail sent, or caused to be sent, to or through the network that makes use of or contains invalid or forged headers, invalid or non-existent domain names, or other means of deceptive addressing will be deemed to be counterfeit. Any attempt to send or cause such counterfeit e-mail to be sent to or through the network is unauthorized. Similarly, e-mail that is relayed from any third party's e-mail servers without the permission of that third party, or which employs similar techniques to hide or obscure the source of the e-mail, is also an unauthorized use of the network. The Board does not authorize the harvesting or collection of network e-mail addresses for the purposes of sending unsolicited e–mail. The Board reserves the right to take all legal and technical steps available to prevent unsolicited bulk e-mail or other unauthorized e-mail from entering, utilizing, or remaining within the network. Nothing in this policy is intended to grant any right to transmit or send e-mail to, or through, the network. The Board's failure to enforce this policy in every instance in which it might have application does not amount to a waiver of its rights.

Unauthorized use of the network in connection with the transmission of unsolicited bulk e-mail, including the transmission of counterfeit e-mail, may result in civil and criminal penalties against the sender and/or possible disciplinary action.

Authorized Use and Training

Pursuant to Policy 7540.04, staff and Board members using the Academy's e-mail system shall acknowledge their review of, and intent to comply with, the Academy's policy on acceptable use and safety by signing and submitting Form 7540.04 F1 annually.

Furthermore, staff and Board members using the Academy's e-mail system shall satisfactorily complete training, pursuant to Policy 7540.04, regarding the proper use and retention of e-mail.

PERSONAL INTERNET ACCOUNT PRIVACY - STUDENTS

Reference: Michigan Internet Privacy Information Act, PA 478 of 2012
MCL 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.

PERSONAL INTERNET ACCOUNT PRIVACY – STAFF

Reference: Michigan Internet Privacy Protection Act, PA 478 of 2012
MCL 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.

ELECTRONIC DATA PROCESSING/INFORMATION SYSTEM DISASTER RECOVERY PLAN

The Board is committed to maintaining and protecting the Academy's Information System. The Board believes that a complete and accurate Information System, including educational, student, fiscal and personnel information, is vital to the Board's ability to deliver uninterrupted educational service to the community it represents. To that end, the ESP is directed to develop, test, and maintain an Electronic Data Processing/Information System Disaster Recovery Plan for use in the event a disaster should disable the Academy's electronic data processing equipment.

The Disaster Recovery Plan may include the following:

A. a reciprocal agreement with a neighboring school or data acquisition site that outlines the scope and costs of reciprocal services (e.g., access to the computer facility of the other site, computer time, personnel assistance, etc.);

B. equipment insurance;

C. a list of the applications used by the Academy;

D. procedures and personnel used to backup all programs and data on a daily, monthly, quarterly, and year-end basis;

E. backup storage off-site;

F. maintenance agreements for hardware and software (including, but not limited to the operating system);

G. a list of vendor contacts to be called for immediate replacement of disabled equipment or corrupted software;

H. as a last resort, the emergency procedures to be used to manually create the Academy's payroll checks and budgetary checks and to manually perform other necessary accounting functions.

ACCESS TO ACADEMY TECHNOLOGY RESOURCES FROM PERSONAL COMMUNICATION DEVICES

The Board permits employees, Board members, contractors, vendors, and agents to use their personal communication devices ("PCDs") to wirelessly access the Academy's technology resources (guest or business networks, servers, projectors, printers, etc.) while they are on-site at any Academy facility. Access to the business/guest network shall require authentication.

For purposes of this policy, "personal communication device" includes computers, tablets (e.g., iPads and similar devices), electronic readers ("e-readers"; e.g., Kindles and similar devices), cell phone (e.g., mobile/cellular telephones), smartphones (e.g., BlackBerry, iPhone, etc.), and/or other web-enabled devices of any type.

If the user wants to access the Academy's technology resources through a hard-wired connection, the user's PCD must first be checked by the Technology Coordinator to verify it meets the established standards for equipment used to access the network.

Technology Coordinator is charged with developing (or, is directed to develop) the necessary standards for connecting PCDs to the Academy's technology resources. The standards shall be available upon request.

The standards shall be designed and enforced to minimize the Board's exposure to damages, including, but not limited to, the loss of sensitive Academy data, illegal access to confidential data, damage to the Academy's intellectual property, damage to the District's public image, and damage to the Academy's critical internal systems, from unauthorized use.

The use of PCDs must be consistent with the established standards for appropriate use as defined in Policy 7540.03 and AG 7540.03 – Student Network and Internet Acceptable Use and Safety, Policy 7540.04 and AG 7540.04 – Staff Network and Internet Acceptable Use and Safety, Policy 5136 and AG 5136 - Personal Communication Device, Policy 7530.02 - Staff Use of Communication Devices. When an individual connects to and uses the Academy's technology resources, s/he must agree to abide by all applicable policies, administrative procedures and laws (e.g., the user will be presented with a "splash screen" that will set forth the terms and conditions under which s/he will be able to access the Academy's technology resource(s); the user will need to accept the stated terms and conditions before being provided with access to the specified technology resource(s)).

In order to comply with the Children's Internet Protection Act ("CIPA"), 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. The Board also utilizes software and/or hardware to monitor online activity to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors.

Any user who violates the established standards and/or the Board's Acceptable Use policy, or who accesses the Academy's technology resources without authorization may be prospectively denied access to the Academy's technology resources. If the violation is committed by a contractor, vendor or agent of the Academy, the contract may be subject to cancellation. Further disciplinary action may be taken if the violation is committed by a student or employee.

The owner of a PCD bears all responsibility and assumes all risk of theft, loss, or damage to, or misuse or unauthorized use of the device while it is on Board property. This provision applies to everyone, regardless of their affiliation or connection to the Academy.

REMOTE ACCESS TO THE ACADEMY'S NETWORK

Access to the Academy's Website (www.madison-academy.org) is encouraged.

The following resources shall be available on the Academy's website:

A. the Academy's calendar of events

B. Powerschool

C. State Transperancy Reporting

D. Board agendas and minutes

The Board encourages staff, parents, students, and community members to check the Academy's website regularly for changes to these resources and for the addition of other resources. Some resources may require a user name and password, or a login procedure due to the personally identifiable nature of the information provided through that resource (e.g., the grade book program and e-mail system). If a user name and password, or login procedure, is necessary to access a resource, information shall be provided on the website explaining who is eligible for a user name and password, how to obtain a user name and password, and detailed instructions concerning the login process.

Access to the Academy Network through Server

Board members, staff members, contractors, vendors, and agents of the Academy, are permitted to use their personally-owned or Academy-owned computer or workstation and/or web-enabled devices of any type to remotely (i.e. away from Academy property and facilities) access the Academy's server and thereby connect to the Academy's Network. This policy is limited to remote access connections that are used to do work on behalf of or for the benefit of the Academy, including, but not limited to, reading or sending e-mail and reviewing Academy-provided intranet web resources.

Each individual granted remote access privileges pursuant to this policy must adhere to the following standards and regulations:

A. his/her device computer/device must have, at the minimum, the anti-virus software specified in the Academy's standards for remote access and connection;

B. the individual may only access the Network using his/her assigned user name and password;

   The individual must not allow other persons, including family members, to use his/her user name and password to login into the Network. The user may not go beyond his/her authorized access.

C. his/her device may not be connected to any other network at the same time s/he is connected to the Network, with the exception of personal networks that are under the complete control of the user;

D. the individual may not access non-school e-mail accounts (e.g. Hotmail, Gmail, Yahoo, AOL, and the like) or other external resources while connected to the Network;

E. his/her device may not, at any time while the individual is using remote access to connect to the Network, be reconfigured for the purpose of split tunneling or dual homing; and

F. use of the Network is contingent upon the individual abiding by the terms and conditions of the Academy's Network and Internet Acceptable Use and Safety policy and procedures.

Users may be required to sign the applicable agreement form (Form 7540.03 F1 or Form 7540.04 F1) prior to being permitted to use remote access.

Additional standards and regulations for remotely accessing and connecting to the Academy network shall be developed and published in AG 7543 - Standards and Regulations for Remote Access and Connection.

Any user who violates this policy may be denied remote access and connection privileges.

Any staff member who violates this policy may be disciplined, up to and including termination; any contractor, vendor or agent who violates this policy may have his/her contract with the Academy terminated; and any student who violates this policy may be disciplined up to and including suspension or expulsion.

ELECTRONIC COMMUNICATIONS

The advancement of technology has provided many new ways for individuals to communicate with one another. These electronic communications include social networking sites, instant messaging, text messaging, e-mailing and photo-sharing, among others. Additional methods of electronic communication can be anticipated as the technology continues to evolve.

However, use of such technology must be approached with caution by ESP. Given the nature of the communications, there is a significant potential both for inappropriate use and for alleged inappropriate use. To protect staff and students, the following restrictions are established:

A. Electronic communications with students should be appropriate in tone, content, and quantity. Stalking, harassment, or other unwelcome behaviors are prohibited, including any type of sexually suggestive comments, photos, or graphics.

B. Electronic communications with other employees should be appropriate in tone, content, and quantity. Stalking, harassment, or other unwelcome behaviors are prohibited.

C. Electronic communications with students are only to occur through Academy maintained e-mail accounts or websites.

The ESP may require the employee to produce records for review when there is reason to believe that this policy has been violated. Records within the Academy's control may be reviewed periodically to assure that this policy is being complied with. These may include Internet logs, cell phone records, or other similar documentation.

Questions regarding acceptable electronic communications or unwelcomed electronic communications from someone associated with the Academy should be submitted to ESP.