

USE OF SOCIAL NETWORKING SITES -- FOR ALL DISTRICT PERSONNEL

The Board of Education has a strong commitment to quality education and the well-being of all pupils, as well as the preservation of the school district's reputation. The Board believes staff members must establish and maintain public trust and confidence and be committed to protecting all pupils attending the school district. In support of the Board's strong commitment to the public's trust and confidence, the Board holds all staff members to the highest level of professional responsibility.

The Commissioner of Education has determined inappropriate conduct outside a staff member's professional responsibilities may determine them as unfit to discharge the duties and functions of their position. Staff members should be advised communications, publications, photographs, and other information appearing on social networking sites deemed inappropriate by the Board could be cause for dismissal of a non-tenured staff member or to certify tenure charges against a tenured staff member to the Commissioner of Education.

Staff members are advised to be concerned and aware such conduct deemed inappropriate may include, but is not limited to, communications and/or publications using e-mails, text-messaging, social networking sites, or any other form of electronic communication that is directed and/or available to pupils or for public display or publication.

While the Board respects the right of staff members to use social networking sites, staff members should recognize they are held to a higher standard than the general public with regard to standards of conduct and ethics. It is important that a staff member's use of these sites does not damage the reputation of the school district, employees, pupils, or their families. Staff members who utilize, post or publish images, photographs, or comments on social networking sites, blogs, or other forms of electronic communication outside their professional responsibilities shall ensure their use, postings, or publications are done with an appropriate level of professionalism and are appropriate conduct for a school staff member. Staff members should exercise care in setting appropriate boundaries between their personal and public online behavior, understanding that what is private in the digital world often has the possibility of becoming public even without their knowledge or consent.

The school district strongly encourages all staff members to carefully review the privacy settings on social networking sites they use and exercise care and good judgment when posting content and information on such sites. Staff members should adhere to the following guidelines, which are consistent with the district's workplace standards on harassment, pupil relationships, conduct, professional communication, and confidentiality.

When using personal social networking sites, school staff members:

1. Should not make statements that would violate any of the district's policies, including its policies concerning discrimination or harassment;
2. Must uphold the district's value of respect for the individual and avoid making defamatory statements about the school district, employees, pupils, or their families;

3. May not disclose any confidential information about the school district or confidential information obtained during the course of his/her employment, about any individual(s) or organization, including pupils and/or their families;
4. Shall not use social networking sites to post any materials of a sexually graphic nature;
5. Shall not use social networking sites to post any materials which promote violence;
6. Shall not use social networking sites which would be detrimental to the mission and function of the district;
7. Are prohibited from using their school district title as well as adding references to the district in any correspondence including, but not limited to, e-mails, postings, blogs, and social networking sites unless the communication is of an official nature and is serving the mission of the district. This prohibition also includes signature lines and personal e-mail accounts;
8. Shall not post updates to their status on any social networking sites during normal working hours including posting of statements or comments on the social networking sites of others during school time unless it involves a school project. Employees must seek approval from the Superintendent of Schools for such use; and
9. Shall not post or publish any information the Commissioner of Education would deem to be inappropriate conduct by a school staff member.

The Policy of this district is to maintain a level of professionalism both during and after the school day. Any publication through any means of electronic communication which is potentially adverse to the operation, morale, or efficiency of the district, will be deemed a violation of this Policy. If the Board or Superintendent believes that a staff member's activity on any social networking site violates the district's policies, the Board or Superintendent may request that the employee cease such activity. Depending on the severity of the incident, the staff member may be subject to disciplinary action.

This Policy has been developed and adopted by this Board to provide guidance and direction to staff members on how to avoid actual and/or the appearance of inappropriate conduct toward pupils and/or the community while using social networking sites.

First Reading: July 19, 2012

HASBROUCK HEIGHTS BOARD OF EDUCATION
Hasbrouck Heights, New Jersey 07604
Regulation

File Code: 4322

Hasbrouck Heights Board of Education

**“Guidelines for the Use of Social Media for
Board Members, Administrators, Teachers,
Staff, Students, Parents/Guardians,
and Community Members”**

Introduction

The rapid growth of social media technologies combined with their ease of use and pervasiveness make them attractive channels of communication. However, these tools also hold the possibility of a host of unintended consequences. To help you identify and avoid potential issues, the Hasbrouck Heights Board of Education and Superintendent have compiled and adapted the guidelines that were published for the University of Michigan in 2010. These guidelines are examples of best practices from various institutions and are intended to help you understand, from a wide range of perspectives, the implications of participation in social media.

Please note that the Hasbrouck Heights Board of Education has adopted Policy 3282 that highlights the consequences that will occur should any staff member disclose confidential information, access and / or post on personal sites during working hours, or publish / post information in any format deemed inappropriate or detrimental to the mission and function of Hasbrouck Heights Schools.

This document was originally developed to provide a set of guidelines in the use of social media applications for the University of Michigan. The Hasbrouck Heights Board of Education has adapted these guidelines for use within the Hasbrouck Heights School District. The original document from the University of Michigan, entitled “Voices of the Staff: Guidelines for the Use of Social Media,” can be found at the following website:

<http://www.compliancebuilding.com/about/publications/social-media-policies/> .

To be Considered When Using Social Media

Applications that allow you to interact with others online (e.g., Facebook, MySpace, etc.) require careful consideration to assess the implications of “friending”, “linking”, “following”, or accepting such a request from another person. For example, there is the potential for misinterpretation of the relationship or the potential of sharing protected information. Relationships such as teacher-student, adult-child, supervisor-subordinate, staff member-student, etc. merit close consideration of the implications and the nature of the social interaction. The following are some guidelines to follow in these cases.

General Guidelines for Posting to Social Media Sites

Sharing school news, disseminating information about school events, or promoting student work, using social media tools is an excellent, low-cost way to engage parents/guardians, students, staff members, and the community. Employees, parents/guardians, students are encouraged to post and share information that is available to the public with family and friends via social networking tools. However, when sharing information that is not a matter of public record, please follow the following guidelines.

- 1) **Maintain Confidentiality:** Do not post confidential or proprietary information about our schools or the School District, about a student or students, about a fellow staff member or staff members, about parents/guardians, about board member or members, or about an administrator or administrators. Use ethical judgment and follow federal and state requirements about confidentiality, such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Family Educational Rights and Privacy Act (FERPA). Please refer to the following board policies regarding communication and confidentiality: 1100, 1140, 4111.1, 4321.
- 2) **Maintain Privacy:** Do not discuss a situation involving named or pictured individuals on a social media site WITHOUT THEIR PERMISSION. As a guideline, do not post anything that you would not present in any public forum.
- 3) **Respect School Time and Property:** It is appropriate to post to FaceBook, MySpace, etc. if your comments are directly related to accomplishing work goals, such as seeking sources for information or working with others to resolve a problem. You should participate in personal social media conversations on your own time.
- 4) **Do No Harm:** Let your internet social networking do no harm to any employee or student or parent/guardian of the School District or to yourself when navigating these social networking sites.
- 5) **Understand Your Personal Responsibility:** Hasbrouck Heights staff members and students and parents/guardians are responsible personally for the content they publish on blogs, wikis, or any other form of user-generated content sites. Be mindful that what you publish will be public for a long time. Protect your privacy and the privacy of others.
- 6) **Be Aware of Your Liability:** You are responsible for what you post on your own site and on the sites of others. Individual bloggers have been held liable for commentary deemed to be copyright infringement, or commentary that is defamatory, proprietary, libelous, or obscene (as defined by the courts). Increasingly, employers are conducting Web searches on job candidates before extending offers of employment. Be sure that what you post will not come back to haunt you or your family members.

- 7) **Maintain Transparency:** The line between professional and personal business is sometimes blurred. Be thoughtful about your posting's content, and the potential audiences of your posts. Be honest about your identity. In your personal posts, you may identify yourself as a staff member of Hasbrouck Heights School District. However, be clear in these posts that your views as an individual are not representative of the Hasbrouck Heights Board of Education or School District.
- 8) **Correct Mistakes:** If you make a mistake, admit and correct the mistake as soon as possible. Be upfront and be quick with your correction. If you are posting to a blog, you may choose to modify any earlier posts – just make clear that you have modified earlier posts in the new posting.
- 9) **Respect Others:** You are more likely to achieve your goals and/or sway others to your beliefs if you are constructive and respectful while discussing a difficult experience or disagreeing with a concept of the opinion(s) of others.
- 10) **Be a Valued Member of the Community:** If you join a social network, make sure you are contributing valuable insights. Don't hijack the discussion and redirect by posting self-promoting information. Self-promoting behavior is viewed negatively and can lead you to being banned from websites or groups.
- 11) **Think Before You Post:** There's no such thing as "private" social media sites. Search engines will turn up posts and pictures years after the publication or the posting has expired. Comments can be forwarded, copied, saved. Archival systems save information even after the deletion of a post. If you feel angry or passionate about a topic, you are wise to delay posting until you are calm and have thought about and chosen your words carefully. Post pictures that you would be comfortable sharing with the general public including current and future employers or your parents or spouse, or your children.

Social Media Guidelines When Posting as an Individual

Hasbrouck Heights School District employees or parents/guardians associated with the Hasbrouck Heights Schools may use social media to supplement traditional press and marketing efforts. Employees are encouraged to share school news and events which are a matter of public record. Linking straight to the information source is an effective way to promote the school district goals and mission and to build community. When you are posting information NOT related to the district, you must be clear that you are not representing the opinion(s) or position(s) of the Board of Education members or School District in your posting(s). While the guidelines below apply to those instances in which there is confusion about your role as an employee, or a student, or a parent/guardian of Hasbrouck Heights Public Schools, these guidelines should be considered for all social media interactions.

- 1) **Be Authentic:** Be honest about your identity. In personal posts, you may identify yourself as an employee or student or parent/guardian of a student of the Hasbrouck Heights Public Schools. However, please be clear that you are sharing personal opinions or viewpoints and not writing/communicating on these social media sites as a representative of the school district.
- 2) **Use a Disclaimer:** If you publish content to any website and the information relates to or is associated with the schools in any way, you must use a disclaimer such as the following: "The postings on this site are my own and do not represent the positions, strategies, viewpoints, or opinions of the Hasbrouck Heights Board of Education or School District."
- 3) **Do Not Make Endorsements:** You are not allowed to use the Hasbrouck Heights Aviators Logo or School District mottos, etc., to promote or endorse any product, cause, political party, or candidate.
- 4) **Take the Higher Ground:** If you identify yourself as a teacher, administrator, parent/guardian, student of Hasbrouck Heights Schools, then readers will associate your comments, beliefs, personal opinions with our school district, even with the disclaimer. Choose respect and dignity over nitpicking and verbal sparring.
- 5) **Don't Use Pseudonyms:** Tracking tools enable supposedly anonymous posts to be traced to the author. Never pretend to be someone else or someone you are not.
- 6) **Protect Your Identity:** While you should be honest about yourself, don't provide personal information that identity thieves could use. Do not use your home address or telephone number. You should consider using a separate email address with only social media sites.
- 7) **Does Your Posting Pass the Publicity Test:** If the content of your posting would not be acceptable face-to-face conversation or conversation over the phone, then the content is not acceptable for a social media site. Ask yourself, "Would I want this information that is generated by me published in a newspaper or newsletter now or in ten years from now?"
- 8) **Respect Your Audience:** Don't use ethnic slurs, personal insults, obscenity, or engage in conduct that would not be acceptable as a teacher or a student or as a parent/guardian or respected community member. Show consideration for others' privacy, especially about topics that are sensitive (i.e., politics or religion).
- 9) **Monitor Comments:** Most people who maintain social media sites welcome comments from others to build credibility and community. However, you may be able to set your site so that you can review and approve comments BEFORE these comments appear as "postings" to your page or site. You may consider setting this parameter to delete spam or block individuals who are offensive or frivolous in their responses to you.

Social Media Guidelines When Posting as a School Community Member

Online collaboration tools provide low-cost communication methods that foster open exchanges and learning. While social media tools are changing the way we work and how we connect with the community and other institutions, the policies for sharing information and for what we can share remain the same. In addition to the general guidelines above, when you are representing Hasbrouck Heights Public Schools on a social media site or in creating a posting to a social media site, please follow these guidelines as well:

- 1) **Seek Approval:** Any messages that act as “the voice” of the school or of the school district must be approved by the building principal and/or superintendent of schools.
- 2) **Be Accurate:** Make sure that you have all the facts before you post. Verify information with a viable source before the posting is published. Cite and link sources to your posting whenever possible, as that’s how you build community.
- 3) **Be Transparent:** If you participate in or maintain a social media site on behalf of the Hasbrouck Heights Public Schools clearly state your role, the goals of the site, and your position. Keep in mind that you are posting as an employee of the school district. Be careful, responsible, and respectful. What you say post or write directly reflects the Hasbrouck Heights Public Schools. Discuss with your supervisor, building principal, or the superintendent of schools the circumstances in which you are empowered to respond directly to users and when you need approval to post, respond to comments, etc., and when you must involve an administrator or the superintendent in postings or responses to comments.
- 4) **Be Timely:** Monitor postings regularly and in a timely fashion. Establish times for postings and updates. The recommended frequency for postings and updates and responses to comments is once or twice weekly. Be sure not to overload the postings with too much information, or readers will stop paying attention.
- 5) **Be Responsible:** What you write is ultimately your responsibility. Participation in social media sites as an employee of Hasbrouck Heights Public Schools or as a student or as a parent/guardian is not a right but an opportunity, so please treat this opportunity seriously, and with respect. You must abide by Hasbrouck Heights Board of Education Policy when posting.
- 6) **Respect Others:** You are more likely to achieve the goals of the site when being constructive and respectful while troubleshooting problems or responding to negative comments. Do not use sarcasm or obscenities ever.
- 7) **Be a Valued, Thoughtful Member:** Make sure you are contributing valuable insights when you post information or post responses as an employee, students, or parent/guardian of the School District. Self-promoting comments must be avoided. If you have a question about a posting or about comments, check with the building principal or superintendent of schools.

Safety and Privacy Tips for Social Media Networking

The internet is open to a world-wide audience. When using social media channels, ask yourself the following questions:

- 1) Did I set my privacy settings to help control who can look at my profile, personal information and photos?
- 2) How much information do I want strangers to know about me? If I provide my cell phone, address, email, class schedule, list of possessions (i.e., CD collection or iTunes list, or YouTube favorites), how might this stranger use this information?
- 3) Are the pictures I'm posting or the comments I'm making the way I would like others to know me?
- 4) What does my profile project about me to future or current employers, colleagues, neighbors, advisors, family members, children, friends?
- 5) If I change my mind about a posting or a picture, have I checked with the social media site's privacy and caching statements? (Removing posts or pictures may be extremely difficult. REMEMBER: Posted pictures and/or material may remain accessible on the internet for many years, even after you've completed the prescribed process for removing such information. Search engines may reveal pictures or postings for years to come.)
- 6) Have I asked permission to use someone else's image or information?
- 7) Am I infringing on the confidentiality and privacy of another?
- 8) Could I be hurting someone with my posting or picture? Am I violating HIPAA or FERPA mandates or Hasbrouck Heights Board of Education policy?
- 9) Does my equipment have spyware and virus protections? (REMEMBER: Some sites collect profile information for spam. Others collect links that may infect your equipment with viruses that track or corrupt data and will infect others with whom you communicate online. Remember to back up your work on an external disk drive in case of destructive attacks.)

***These guidelines have been adapted from the social networking guidelines from the University of Michigan
January 2010, revised July 2012.***

See **www.voices.umich.edu** .

Highlighted areas to be removed; **Bolded areas to be added**

ACCEPTABLE USE OF COMPUTER NETWORKS/
COMPUTERS AND RESOURCES FOR ALL DISTRICT PERSONNEL

The Board of Education recognizes ~~that as telecommunications and other~~ new technologies shift the manner in which information is accessed, communicated, and transferred; **these** ~~that these~~ changes will alter the nature of teaching and learning. Access to ~~telecommunications~~ **technology** will allow pupils to explore databases, libraries, Internet sites, **and** bulletin boards ~~and the like~~ while exchanging information with individuals throughout the world. The Board supports access by pupils to **these** information sources but reserves the right to limit in-school use to materials appropriate **for** ~~to~~ educational purposes. The Board directs the Superintendent to effect training of teaching staff members in skills appropriate to analyzing and evaluating such resources as to appropriateness for educational purposes.

The Board also recognizes ~~that telecommunications~~ **technology** ~~will~~ allows pupils access to information sources that have not been pre-screened by educators using Board approved standards. The Board therefore adopts the following standards of conduct for the use of computer networks and declares unethical, unacceptable, or illegal behavior as just cause for taking disciplinary action, limiting or revoking network access privileges, and/or instituting legal action.

The Board provides access to computer networks/computers for educational purposes only. The Board retains the right to restrict or terminate pupil access to ~~the~~ computer networks/computers at any time, for any reason. **School** ~~The Board retains the right to have~~ district personnel **will** monitor networks **and** ~~online~~ activity, ~~in any form necessary,~~ to maintain the integrity of the networks, **and** ~~ensure their~~ **its** proper use, **and ensure compliance with Federal and State laws that regulate Internet safety.**

Standards for Use of Computer Networks

Any individual engaging in the following actions when using computer networks/computers shall be subject to discipline or legal action:

- A. Using the computer network(s)/computers for illegal, inappropriate or obscene purposes, or in support of such activities. Illegal activities are defined as activities that violate Federal, State, local laws and regulations. Inappropriate activities are defined as those that violate the intended use of the networks. Obscene activities shall be defined as a violation of generally accepted social standards for use of publicly owned and operated communication vehicles.
- B. Using the computer network(s)/computers to violate copyrights, institutional or third party copyrights, license agreements or other contracts.
- C. Using the computer network(s) in a manner that:
 - 1. Intentionally disrupts network traffic or crashes the network;
 - 2. Degrades or disrupts equipment or system performance;

3. Uses the computing resources of the school district for commercial purposes, financial gain, or fraud;
4. Steals data or other intellectual property;
5. Gains or seeks unauthorized access to the files of others or vandalizes the data of another **person user**;
6. Gains or seeks unauthorized access to resources or entities;
7. Forges electronic mail messages or uses an account owned by others;
8. Invades privacy of others;
9. Posts anonymous messages;
10. Possesses any data which is a violation of this **P**olicy; and/or
11. Engages in other activities that do not advance the educational purposes for which computer networks/computers are provided.

Internet Safety Protection

As a condition for receipt of certain Federal funding, ~~t~~The school district **shall be** is in compliance with the Children's Internet Protection Act, **the Neighborhood Children's Internet Protection Act**, and has installed technology protection measures for all computers in the school district, including computers in media centers/libraries. **The technology protection must** ~~that~~ block and/or filter **material and** visual depictions that are obscene as defined in Section 1460 of Title 18, United States Code; child pornography, as defined in Section 2256 of Title 18, United States Code; are harmful to minors including any pictures, images, graphic image file or other **material or** visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or depicts, describes, or represents in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

~~The school district will certify on an annual basis, that the schools, including media centers/libraries, in the district are in compliance with the Children's Internet Protection Act and the school district enforces the requirements of this policy.~~

This Policy also establishes Internet safety policy and procedures in the district as required in the Neighborhood Children's Internet Protection Act. Policy 2361 addresses access by minors to inappropriate matter on the Internet and World Wide Web; the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; unauthorized access, including "hacking" and other unlawful activities by minors online; unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and measures designed to restrict minors' access to materials harmful to minors.

Notwithstanding blocking and/or filtering the **material and** visual depictions prohibited in the Children's Internet Protection Act **and the Neighborhood Children's Internet Protection Act**, the Board shall determine other Internet material that is inappropriate for minors.

In accordance with the provisions of the Children's Internet Protection Act, the Superintendent of Schools or designee will develop and ensure education is provided to every pupil regarding appropriate online behavior, including pupils interacting with other individuals on social networking sites and/or chat rooms, and cyberbullying awareness and response.

The Board will provide reasonable public notice and will hold one annual public hearing during a regular monthly Bboard meeting or during a designated special Bboard meeting to address and receive public community input on the Internet safety policy - Policy and Regulation 2361. **Any changes in Policy and Regulation 2361 since the previous year's annual public hearing will also be discussed at a meeting following the annual public hearing.**

The school district will certify on an annual basis, that the schools, including media centers/libraries in the district, are in compliance with the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act and the school district enforces the requirements of these Acts and this Policy.

Consent Requirement

No pupil shall be allowed to use the **school districts'** computer networks/computers and the Internet unless they ~~shall~~ have filed with **the** _____ **(individual or office)** a consent form signed by the pupil and his/her parent(s) or legal guardian(s).

Violations

Individuals violating this ~~P~~olicy shall be subject to the consequences as indicated in Regulation ~~N~~o. 2361 and other appropriate discipline, which includes but are not limited to:

1. Use of the network only under direct supervision;
2. Suspension of network privileges;
3. Revocation of network privileges;
4. Suspension of computer privileges;
5. Revocation of computer privileges;
6. Suspension from school;
7. Expulsion from school; and/or
8. Legal action and prosecution by the authorities.

N.J.S.A. 2A:38A-3

Federal Communications Commission: Children's Internet Protection Act-

Federal Communications Commission: Neighborhood Children's Internet Protection Act

Approved: January 28, 2010

Revised (First Reading): July 19, 2012

Highlighted areas to be removed; **Bolded areas to be added**

ACCEPTABLE USE OF COMPUTER NETWORKS/
COMPUTERS AND RESOURCES FOR ALL DISTRICT PERSONNEL

The school district provides computer equipment, computer services, and Internet access to its pupils and staff for educational purposes only. The purpose of providing technology resources is to improve learning and teaching through research, teacher training, collaboration, dissemination and the use of global communication resources.

For the purpose of this Policy and Regulation, “computer networks/computers” includes, but is not limited to, the school district’s computer networks, computer servers, computers, other computer hardware and software, Internet equipment and access, and any other computer related equipment.

For the purpose of this Policy and Regulation, “school district personnel” shall be the person(s) designated by the Superintendent of Schools to oversee and coordinate the school district’s computer networks/computer systems. School district personnel will ~~The “system administrators” referred to herein as employees of the school district who administer the school district computer network/computers and the system administrators reserve the right to monitor~~ **networks and online activity, in any form necessary, to maintain the integrity of the networks, ensure proper use, and to be in compliance with Federal and State laws that regulate Internet safety all activity on network/computer facilities/computers.**

Due to ~~Because of~~ the complex association between ~~so many~~ government agencies and computer networks/computers **and the requirements of Federal and State laws**, the end user of ~~these~~ **the school district’s** computer networks/computers must adhere to strict regulations. Regulations are provided ~~here to assure so that~~ staff, community, and pupils, users and the parent(s) or legal guardian(s) of pupils are aware of their responsibilities. The school district may modify these regulations at any time ~~by publishing modified regulations on the network and elsewhere.~~ The signatures of the pupil and his/her parent(s) or legal guardian(s) on ~~a~~ **the** district-approved ~~Ce~~consent and ~~W~~waiver ~~A~~agreement are legally binding and indicate ~~that~~ the parties have read the terms and conditions carefully, understand their significance, and agree to abide by the rules **and regulations** established under Policy and Regulation No. 2361.

Pupils are responsible for **acceptable and appropriate** ~~good~~ behavior **and conduct** on school district computer networks/computers ~~just as they are in a classroom or a school hallway.~~ Communications on the computer networks/computers are often public in nature **and:** ~~p~~Policies and ~~r~~Regulations governing **appropriate** behavior and communications apply. The school district’s networks, Internet access, and computers are provided for pupils to conduct research, **complete school assignments**, and communicate with others. Access to computer networks ~~services~~/computers is given to pupils who agree to act in a considerate, **appropriate**, and responsible manner. Parent(s) or legal guardian(s) permission is required **for a pupil to access the school district’s computer networks/computers.** ~~Access is a privilege not a right.~~ Access entails responsibility **and:** ~~I~~Individual users of the district computer networks/computers are responsible for their behavior and communications over the computer networks/computers. It is presumed ~~that~~ users will comply with district standards and will honor the agreements they have signed **and the permission they have been granted.** Beyond the clarification of such standards, the district is not responsible for the actions of individuals utilizing the computer networks/computers who violate the policies and regulations of the Board.

Computer networks/computer storage areas shall be treated in the same manner as other school storage facilities. **School district personnel** ~~Computer network/computer administrators~~ may review files and communications to maintain system integrity, ~~and ensure that~~ **confirm** users are using the system responsibly, **and ensure compliance with Federal and State laws that regulate Internet safety.** ~~Therefore, Users no person should not expect that~~ files stored on district servers will ~~always~~ be private or confidential.

~~Within reason, freedom of speech and access to information will be honored. During school, teachers of younger pupils will guide them toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media. As outlined in Board policy and procedures on pupil rights and responsibilities, copies of these are available in school offices. The following prohibited bBehavior and/or conduct using the school district's networks/computers, includesing but is not limited to, the following are prohibited:~~

1. Sending or displaying offensive messages or pictures;
2. Using obscene language and/or accessing **material or** visual depictions that are obscene as defined in section 1460 of Title 18, United States Code;
3. Using or accessing **material or** visual depictions that are child pornography, as defined in section 2256 of Title 18, United States Code;
4. Using or accessing **material or** visual depictions that are harmful to minors including any pictures, images, graphic image files or other **material or** visual depictions that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or
5. ~~Depictsing, describesing, or representsing~~ in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors-;
6. **Cyberbullying;**
7. **Inappropriate online behavior, including inappropriate interaction with other individuals on social networking sites and in chat rooms;**
86. Harassing, insulting, or attacking others;
97. Damaging computers, computer systems, or computer networks/computers;
108. Violating copyright laws;
119. Using another's password;
1210. Trespassing in another's folders, work or files;
1311. Intentionally wasting limited resources;
1412. Employing the computer networks/computers for commercial purposes; and/or
1513. Engaging in other activities that do not advance the educational purposes for which computer networks/computers are provided.

INTERNET SAFETY

Compliance with Children's Internet Protection Act

As a condition for receipt of certain Federal funding, tThe school district has technology protection measures for all computers in the school district, including computers in media centers/libraries, that block and/or filter **material or** visual depictions that are obscene, child pornography and harmful to minors as defined in 2, 3, ~~and~~ 4, **5, 6, and 7** above and in the Children's Internet Protection Act. The school district will certify the schools in the district, including media centers/libraries are in compliance with the Children's Internet Protection Act and the district **complies with and enforces Policy and Regulation 2361.**

Compliance with Neighborhood Children's Internet Protection Act

Policy 2361 and this Regulation establishes an Internet safety **protection** policy and procedures to address:

1. Access by minors to inappropriate matter on the Internet and World Wide Web;
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
3. Unauthorized access, including "hacking" and other unlawful activities by minors online;
4. **Cyberbullying;**
5. **Inappropriate online behavior, including inappropriate interaction with other individuals on social networking sites and in chat rooms;**
64. Unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and
75. Measures designed to restrict minors' access to materials harmful to minors.

Notwithstanding the **material or** visual depictions defined in the Children's Internet Protection Act **and the Neighborhood Children's Internet Protection Act** ~~and as defined in 2, 3, and 4 above~~, the Board shall determine Internet material that is inappropriate for minors.

The Board will provide reasonable public notice and will hold one annual public hearing during a regular monthly Board meeting or during a designated special Board meeting to address and receive public community input on the Internet safety **protection** policy - Policy and Regulation 2361. **Any changes in Policy and Regulation 2361 since the previous year's annual public hearing will also be discussed at a meeting following the annual public hearing.**

Information Content and Uses of the System

Pupils may ~~Users agree~~ not to publish on or over the system any information which violates or infringes upon the rights of any other person or any information which would be abusive, profane, or sexually offensive to an **reasonable average** person, or which, without the approval of the **Superintendent of Schools or designated school district personnel** ~~system administrators~~, contains any advertising or any solicitation of ~~other members~~ to use goods or services. **A pupil cannot** ~~The user agrees not to use the~~

facilities and capabilities of the system to conduct any business or solicit the performance of any activity, which is prohibited by law.

Because the school district provides, through connection to the Internet, access to other computer systems around the world, pupils and their parent(s) or legal guardian(s) **should be advised** ~~understand that~~ the Board and ~~system administrators~~ **school district personnel** have no control over content. While most of the content available on the Internet is ~~innocuous~~ **not offensive** and much of it is a valuable educational resource, some objectionable material exists. **Even though** ~~t~~The Board ~~will~~ provides pupils access to Internet resources **through the district's computer networks/computers with installed appropriate technology protection measures**, parents and pupils must be advised ~~only in supervised environments and has taken steps to lock out objectionable areas to the extent possible, but potential dangers remain~~ **and offensive material may be accessed notwithstanding the technology protection measures taken by the school district.**

Pupils and their parent(s) or legal guardian(s) are advised ~~that~~ some systems **and Internet sites** may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal **or offensive** material. The Board and ~~the~~ **school district personnel** ~~system administrators~~ do not condone the use of such materials and do not permit usage of such materials in the school environment. Parent(s) or legal guardian(s) having **Internet access available to their children at home** ~~accounts on the system~~ should be aware of the existence of such materials and monitor **their child's access to the school district system at home** ~~usage of the school district computer network~~. Pupils knowingly bringing such materials **prohibited by Policy and Regulation 2361** into the school environment will be disciplined in accordance with Board policies and regulations and such activities may result in termination of such pupils' accounts **or access** on the **school district's** computer networks and their independent use of computers.

On-line Conduct

Any action by a pupil or other user of the school district's computer networks/computers that is determined by **school district personnel** ~~a system administrator~~ to constitute an inappropriate use of **the district's** computer networks/computers ~~resources~~ or to improperly restrict or inhibit other **persons** ~~members~~ from using and enjoying those resources is strictly prohibited and may result in limitation on or termination of an offending **person's** ~~member's~~ **access** ~~account~~ and other **consequences** ~~action~~ in compliance with ~~the~~ Board policy and regulation. The user specifically agrees not to submit, publish, or display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal **or offensive** material; nor shall a user encourage the use, sale, or distribution of controlled substances. Transmission of material, information or software in violation of any local, State or Federal law is also prohibited and is a breach of the Consent and Waiver Agreement.

Pupils ~~Users~~ and their parent(s) or legal guardian(s) specifically agree to indemnify the ~~sSchool dDistrict~~ and **school district personnel** ~~the system administrators~~ for any losses, costs, or damages, including reasonable attorneys' fees incurred by the Board relating to, or arising out of any breach of this section by the **pupil user**.

Computer networks/computer resources are to be used by the **pupil user** for his/her educational use only; commercial uses are strictly prohibited.

Software Libraries on the Network

Software libraries on **or through** the **school district's** networks are provided to pupils as an educational resource. No pupil may install, upload, or download software without the expressed consent of **appropriate school district personnel** ~~the system administrator~~. Any software having the purpose of damaging **another person's** ~~other members'~~ accounts **or information** on the school district computer

networks/computers (e.g., computer viruses) is specifically prohibited. **School district personnel** ~~The system administrators, at their sole discretion,~~ reserve the rights to refuse posting of files and to remove files. **School district personnel** ~~The system administrators, at their sole discretion,~~ further reserve the right to immediately limit usage or terminate the **pupil's access account** or take other action consistent with the Board's policies and regulations of a **pupil member** who misuses the software libraries.

Copyrighted Material

Copyrighted material must not be placed on any system connected to the computer networks/computers without **authorization** ~~the author's specific written permission. Only the owner(s) or persons they specifically authorize may upload copyrighted material to the system.~~ **Pupils Members** may download copyrighted material for their own use in accordance with Policy and Regulation Nos. 2531,— **Use of Copying Copyrighted Materials.** Any **pupil member** may **only** ~~also nonecommercially~~ redistribute a copyrighted program with the expressed written permission of the owner or authorized person. Permission must be specified in the document, on the system, or must be obtained directly from the author **or authorized source.**

Public Posting Areas (Message Boards,~~Usenet Groups~~ **Blogs, Etc.**)

~~Usenet Messages~~ are posted from systems connected to the Internet around the world and ~~the school district personnel system administrators~~ have no control of the content of messages posted from these other systems. To best utilize system resources, **school district personnel** ~~the system administrators~~ will determine **message boards, blogs, etc.** ~~which Usenet groups that~~ are most applicable to the educational needs of the school district and will **permit access to carry these groups sites through on** the school district computer networks. **School district personnel** ~~The system administrators, at their sole discretion,~~ may remove messages ~~posted locally~~ that are deemed to be unacceptable or in violation of the Board policies and regulations. **School district personnel** ~~The system administrators, at their sole discretion,~~ further reserve the right to immediately terminate the **access account** of a **pupil member** who misuses these **public posting areas** ~~message boards or Usenet groups.~~

Real-time, Interactive, Communication Areas

School district personnel ~~The system administrators, at their sole discretion,~~ reserve the right to monitor and immediately limit the use of the computer networks/computers or terminate the **access account** of a **pupil member** who misuses real-time conference features (talk/chat/Internet relay chat).

Electronic Mail

Electronic mail ("eE-mail") is an electronic message sent by or to a **person member** in correspondence with another person having Internet mail access. **The school district may or may not establish pupil email accounts. In the event the district provides email accounts,** ~~a~~All messages sent and received on the school district computer networks/computers must have an educational purpose and are subject to review. Messages received by a **district-provided email account** ~~the system~~ are retained on the system until deleted by the **pupil recipient** or for a **period of time determined by the district** ~~maximum of fifteen days.~~ A canceled account will not retain its eE-mails. **Pupils Members** are expected to remove old messages within fifteen days or **school district personnel** ~~the system administrators~~ may remove such messages. **School district personnel** ~~The system administrators~~ may inspect the contents of eE-mails sent by a **pupil one member** to an addressee, or disclose such contents to other than the sender or a recipient when required to do so by the ~~Board~~ policy, regulation, or other laws and regulations of the State and Federal governments. The Board reserves the right to cooperate fully with local, State, or Federal officials in any investigation concerning or relating to any eE-mail transmitted **or any other information** on the school district computer networks/computers.

Disk Usage

The ~~district system administrators~~ reserves the right to **establish maximum storage space a pupil receives** ~~set quotas for disk usage on the school district's system~~. A **pupil member** who exceeds his/her quota of **storage disk space** will be advised to delete files to return to compliance with **the predetermined amount of storage space quotas**. A **pupil member** who remains in noncompliance of **the storage disk space quotas allotment** after seven school days of notification ~~may will~~ have their files removed ~~from the school district's system by a system administrator~~.

Security

Security on any computer system is a high priority, especially when the system involves many users. If a **pupil member** ~~feels that he/she can~~ identifies a security problem on the computer networks/computers, the **pupil member** must notify **the appropriate school district staff member a system administrator**. The **pupil member** should not inform **other** individuals ~~other than the system administrators or other designated members of the school district staff~~ of a security problem. ~~Professional staff may allow individuals who are not members to access the system through the staff personal account as long as the staff person does not disclose the password of the account to the individuals and understands that the staff person assumes responsibility for the actions of individuals using his/her account. Members may not otherwise allow others to use their account and password.~~ Passwords **provided to pupils by the district for access to the district's computer networks/computers or developed by the pupil for access to an Internet site to the system** should not be easily guessable by others **or shared with other pupils**, nor should they be words, which could be found in a dictionary. Attempts to log in to the system using either another **pupil's member's or person's** account ~~er as a system administrator will~~ **may** result in termination of the account **or access**. A **pupil** ~~Members~~ should immediately notify **the Principal or designee a system administrator** if a password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their account. Any **pupil member** identified as a security risk will have limitations placed on usage of the computer networks/computers or may be terminated as a user and be subject to other disciplinary action.

Vandalism

Vandalism to any school district owned computer networks/computers may will result in cancellation of system privileges and other disciplinary measures in compliance with the ~~d~~District's discipline code. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the system, or any of the agencies or other computer networks/computers that are connected to the Internet backbone or of doing intentional damage to hardware or software on the system. This includes, but is not limited to, the uploading or creation of computer viruses.

Printing

The printing facilities of the computer networks/computers should be used judiciously. **Unauthorized p**Printing for other than educational purposes is prohibited.

Internet Sites and the World Wide Web

Designated school district personnel ~~The system administrator~~ may establish an Internet site(s) on the World Wide Web or other Internet locations. Such sites shall be administered and supervised by **designated school**

~~district personnel the system administrator,~~ who shall ensure that the content of the site complies with Federal, State, and local laws and regulations as well as Board policies and regulations.

Violations

Violations of the Acceptable Use of Computer Networks/Computers and Resources **Policy and Regulation** may result in a loss of access as well as other disciplinary or legal action. Disciplinary action shall be taken as indicated in Policy and/or Regulation, ~~Nes. 2361,-~~Acceptable Use of Computer Networks/Computers and Resources, ~~Nes. 5600,-~~Pupil Discipline/**Code of Conduct**, ~~Nes. 5610,-~~Suspension and ~~Nes. 5620,-~~Expulsion as well as possible legal action and reports to the legal authorities and entities.

Determination of ~~C~~onsequences for Violations

The particular consequences for violations of this ~~P~~olicy shall be determined by the ~~(individual responsible for computer network/computers)~~ **Superintendent and/or Principal or designee** in matters relating to the use of computer networks/computers and by the Principal in matters of school suspension. The Superintendent or designee and the Board shall determine when school expulsion and/or legal action or actions by the authorities ~~is are~~ the appropriate course of action.

Individuals violating this ~~P~~olicy shall be subject to the consequences as indicated in **Board Policy and Regulation Nes. 2361** and other appropriate discipline, which includes but is not limited to:

1. Use of ~~c~~Computer ~~n~~etworks/~~c~~Computers only under direct supervision;
2. Suspension of network privileges;
3. Revocation of network privileges;
4. Suspension of computer privileges;
5. Revocation of computer privileges;
6. Suspension from school;
7. Expulsion from school; and/or
8. Legal action and prosecution by the authorities.

Decisions of the _____ ~~(individual responsible for computer networks/computers)~~ may be ~~appealed in accordance with Policy No. 5710 Pupil Grievances.~~

Approved: January 28, 2010
Revised (First Reading): July 19, 2012