Book District Policies

Section 5: General Personnel

Title Acceptable Use Guidelines for Electronic Communications

Number 5.125

Status Active

Legal

Adopted February 4, 2013

For Electronic Communications in Conducting Aurora West School District 129

Business for Employees/Volunteers

Aurora West School District 129 District employees/volunteers have been utilizing technology for many years in delivering upon our mission to educate students to be self-directed, collaborative learners and workers, critical thinkers, top-notch producers, and contributors to their communities. In addition to their educational pursuits, today's students, and those coming to us in future years, are deeply immersed in electronic forms of communications and associated technologies for their daily interaction with friends, family, community and larger social networks.

As District employees/volunteers, many of us have utilized technologies such as email, websites, blogs, text messaging and use of social media websites such as Facebook, Twitter, and more, to communicate with similar groups for personal interactions. These forms of communication are dynamic, mobile, and quickly reach their targeted audience through technologies that have become an integral part of our lives.

As these technologies continue to advance at a rapid pace, they can become sources of significant benefit to our educational process when integrated into our District's educational delivery model. While continual evolution will undoubtedly occur in this area, it is our goal in issuing these guidelines to increase awareness and understanding of these technologies as well as ensure that their use for District business meets the public and professional standards for communicating with students that we set for ourselves here in West Aurora School District 129.

These guidelines are designed for the purpose of:

- **Clarifying acceptable ways to use electronic communication tools when communicating with students, peers, and community members for District-related business.**
- **Raising awareness of the positive and negative outcomes that may result in using these tools when interacting with the targeted audience.**

- **Establishing the appropriate levels of approval for the use and integration of these technologies for educational benefits aligned with our District mission.**

This document is coupled with a visual matrix that uses color coding to help clarify our District position related to various forms of electronic communication. In the visual matrix, individuals or groups are categorized into either communication originators or communication receivers (also referred to as the targeted audience) to help with the interpretation of the guidelines.

Social media is an evolving tool, and this document is intended to evolve with it. While the general "TAPE" standard outlined below applies to all electronic communications, this document will be updated periodically when new, major social media tools appear.

Nothing in these guidelines should be construed as limiting or abridging any right granted or provided District 129 staff members under Section 7 of the National Labor Relations Act or the Illinois Education Labor Relations Act including any rights of self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing and to engage in other protected activities for the purpose of collective bargaining.

When preparing to communicate with the targeted audience electronically regardless of the medium used, the communication originators should always be mindful of the following key principals, which we refer to as the **TAPE** standards.

Is this communication **Transparent**? – All electronic communication between District employees and students to the targeted audience should be transparent, with the knowledge that the communication is inherently not private, and could be viewed by others. As a public school District, we are expected to maintain openness, visibility, and accountability with regard to all communications.

Is this communication **Accessible**? – All electronic communication between District employees and students should be considered a matter of record, and/or may be accessible by others, and is subject to FOIA (Freedom Of Information Act) requests, etc.

Is this communication **Professional**? – All electronic communication from District employees to the targeted audience should be written or communicated in a professional manner representing West Aurora School District 129. This includes word choices, tone, grammar, and subject matter that model the standards, integrity, and excellence that are expected from every District employee. When communicating district business, be mindful to choose words that are courteous, conscientious, and generally businesslike in manner.

Is the communication **Ethical**? – All electronic communication originating from District employees to their intended audience should be free from harassing or intimidating (bullying and/or cyber bullying) content. Also reference Illinois School Code as described in PA096-0952.

Online media can be viewed as extensions of our classroom and administrative environments when used for conducting District business or activities. Conduct that is deemed inappropriate within the classroom,

school or any District environment should also be deemed inappropriate when using any of these technologies for District communications.

District employees/volunteers should always consider the age appropriateness of the social media or network environments being considered for use within our educational system. Some social media environments (such as Facebook) are not accessible by students under the age of thirteen. Others require parental permission for minors under thirteen. District employees are required to always abide by the age appropriateness of the tools utilized as well as the specific approval procedures required by these guidelines.

Educational professionals and staff members of District 129 will be accountable for complying with the standards set forth for electronic communications set forth herein. Violations of the policy will be subject to disciplinary action up to and including termination.

Explanation of Terms

With the rapid development of new communication technologies, these guidelines are designed to allow flexibility for future technological advancements along with providing clear expectations for existing platforms. To that end an explanation of terms to be used within this document follows:

District Related Communications – Communications that are subject to FOIA requests and are specifically pertinent to the ongoing operations of District 129 and the provision of educational services to the community.

District Employee – Refers to a person who is employed by the District and is being paid for the work they perform on behalf of the District.

Student (K-12) – Identified as a person who is actively enrolled as a student within the District and receiving educational services.

Individual parent/guardian – Indicates a person who is either a parent or designated guardian to any student in District 129.

District Volunteer(s) – Individuals or groups of individuals who are not District Employees but are acting on behalf of District 129 in a service capacity.

General Public – Refers to the community at large.

District Email – Enterprise email system (Microsoft Office365) or any email system licensed by the District and configured for each employee, student, or to whomever access to this system is granted under District operational procedures.

District Standard Applications – Applications licensed, approved, managed and sponsored by the District for communication, collaboration such as: School Messenger, Eschool Home Access Center, etc.

Facebook – A large and well-known example of one of the many social networking sites. Each user posts a profile and "connects" with others via "friend requests." Facebook specifically requires that members be thirteen year old, or older, and thus is never an appropriate tool for communicating with students younger than thirteen years old.

Freedom Of Information Act – A set of laws that gives citizens the right to request full or partial disclosure of records held by governmental bodies to ensure governmental transparency and accountability.

Non-District Email – Any other email system than the District-provided solution mentioned under District Email above, such as: Gmail, Yahoo, and Hotmail.

Permissions Denial Form – A form signed by parents informing the District that they do not wish District Staff members to contact their student using electronic means, including emails, texts, and social media vehicles. A parent or guardian's choice to allow contact via these means should not be construed as permission to "friend" students, or otherwise contact students, via personal social media accounts or pages. Student should only be contacted via professional pages or accounts.

Social Media – A media that delivers content and allows readers, viewers, and listeners the ability to participate and interact with other users. Blogs, forums, wikis, video streaming sites (YouTube) and chat rooms are examples because they include an interactive component.

Social Networking – Describes online tools that connect individuals or groups of people on the Web. Users can create profiles, create and join groups, and build applications for others to use. Social networking sites include, but are not limited to Facebook (see above), Twitter, LinkedIn and external audio / video conferencing tools such as Skype.

Student Information System – One of the key District Standard Applications providing operational functionality required to administer day-to-day District school related operations such as enrollment, registration, grade book, attendance, discipline, parent and student portal, etc.

Text Messaging – Written electronic messages sent from one user to another user or group of users, generally by using mobile devices.

Twitter – A social networking tool using short electronic messages similar to texting to communicate information or quick updates accessible from an internet browser (PC, mobile device, etc.)

Voice Telecommunications – The use of cellular or other telephone devices to communicate verbally.

Expectations for Use of Electronic Communications

District 129 Email – Use of District email is the preferred method for District Employees and/or students to whom District email addresses have been issued to communicate directly with the targeted audience for any District-related business needs. It is also expected and acceptable that individuals who have not been issued District email accounts will send email communications to a District employee's approved

District email account from their own external email systems as needed. Should the District email offering be extending to students, this will also be an acceptable and encouraged form of electronic communication. District email is provided for District-related business, and should not be used for personal matters, mass emails, or solicitation of any kind.

Voice Telecommunications – Existing District policy stipulates that student mobile phones are currently not integrated into the District's educational processes and must be silenced and stored out of sight during the academic day. However, voice telecommunications can be an acceptable channel for communications both during and after school hours based on the guidelines outlined below. For all voice communications, proper professional ethics should always be followed.

District Employees, Parents/Guardians, District Volunteers and General Public:

The District does allow voice communications between District Employees, Parents, District volunteers and the general public as a vehicle to conduct District-related business.

Examples: 1) A District employee places a telephone call to a parent to respond to a concern regarding student performance; 2) A Home and School volunteer places a telephone call to a District employee to coordinate a school event; 3) A parent/guardian of a District student telephones a District employee to provide feedback on a recently issued District communication.

Primary (K-5) Grades:

The District does not allow voice communications originating with District employees or District volunteers to students at these levels. Instead, District employees and District volunteers should contact the student's parents or guardians directly. Conversely, students at these levels should not call District employees or District volunteers directly, but instead have a parent or guardian do so.

Example: 1) A teacher has a referral she would like to share with a K-5 student regarding tutoring. The teacher places a telephone call directly to the student's parent/guardian to share this information; 2) A teacher supervises an after school activity. The ending time of the meeting the next day is being changed. The teacher calls the K-5 student's home and leaves a message with the parents of the child; 3) A K -5 student would like information from the school principal related to a school program. The student calls the principal directly. The principal asks to speak with the student's parents before continuing the conversation.

Secondary (6-12) Grades:

The District does allow voice communications between District employees or District Volunteers and students at these levels provided the student's parents/guardians have not signed the District's Permissions Denial form, and that the communication is specifically conducted with the intent to conduct District-related business.

Example: 1) A student calls a teacher at the school after school hours to set up an appointment to utilize classroom resources for a student team meeting. The student leaves a voicemail for the teacher, who confirms that the students' parents/guardians have not signed the Permissions Denial form, and then telephones the student back at home with confirmation; 2) The coach of a high school sports team has a time change for practice. The coach calls the team captains (6-12 students) asking them to inform the team of the change, after confirming that the captain's parents/guardians have not signed the Permissions Denial form; 3) A PTA member calls a student who is a leader for a school-based club to organize a presentation for an upcoming activity, after confirming that the student's parents/guardians have not signed the Permissions Denial form.

District-Standard Applications – The use of these District-provided tools is strongly encouraged across all levels. Their accessibility is ubiquitous and content is highly transparent. With some of these tools, District employees, District volunteers, students and parents/guardians can gain access to enhanced communication tools and provide immediate and impactful feedback to students and parents.

Examples: 1) A parent/ guardian logs onto the Home Access Center of the District student information system to view their student's grade performance; 2) Students log onto a District library system to view library card catalog contents; 3) Teachers log in to Discovery Education to display education videos to their class; 4) Students log into Read180 to gain access to supplemental material; 5) A building Office Professional updates the school's calendar

Social Media / Social Networking – As indicated on the attached Acceptable Use Guidelines for Electronic Communications matrix, the use of social media / social networking is approved for contacting students whose parents have not signed a Permissions Denial form. Social media and networking should never be used for interpersonal (one to one) District-related communications subject to FOIA regulations and concerning confidential student and/or parent/guardian information. The intent of social media and networking usage should be for approved group-to-group or group-to-general public communications, or conversations carried out collaboratively between individuals, but in full view of the community using the social media tool, such as is the case in blogs. The guidelines below summarize the expectations in this area

General Guidelines for All Social Media/Networking Communications

Unless authorized by the District, District Employees and Volunteers should never post confidential student or employee information online, or in any other electronic format excepting District Email. If there are any questions about the confidentiality of information to be posted, seek clarification from the administrator at your location. District employees are also required to monitor closely the contents of any social media or networking tool in use for educational purposes. Specifically, District Employees should monitor social media and networking tools being used for classroom purposes to ensure that the communications occurring therein are of an appropriate nature for the age group and class for which the tool is employed. Managing social media sites is much like monitoring behavior in a classroom, thus the

posting of content by students should be structured, reviewed prior to posting, and monitored to ensure the appropriateness of content.

District employees and District volunteers should not post or use pictures or videos of individual student without prior approval. District employees and district volunteers should not post pictures or videos of individual students along with their names without prior approval.

Group photos or videos that do not identify individual students are acceptable if the students imaged do not have a Permissions Denial form on file with District 129.

District Employees, District Volunteers

The District does not recommend the use of social media or networking sites by District employees or District Volunteers for the purpose of communicating or conducting District business on an individual basis between District employees, individual District volunteers and Parents/guardians. Such sites are less secure than District email, and are not to be used when sensitive information regarding students or parents is communicated. Such communications are also subject to FOIA requests, and District employees should take care to ensure that communications that are subject to FOIA occur via District email. District employees and District Volunteers should use District email or other District communication tools if there is any possibility that confidential student or parent information may be compromised on public, social media sites.

It is also requested that parents/guardians avoid using these technologies for communicating District-related business to individual District employees, but instead use either email to District employees, voice communications, District Standard applications, or text messaging as outlined in the matrix provided.

Social media and networking may be used by District employees or District volunteers to communicate with broader audiences (other than individual). In no circumstances should District employees or volunteers create Facebook or other social media pages using false identities. This constitutes a breach of professional ethics and clearly violates the guidelines laid out in the TAPE standards above.

Examples: 1) Home and school or PTA/PTO organizations create a Facebook Fan Page to promote school events and increase visibility among parents); 2) A school Art department creates a Shutterfly page where student works can be viewed by family and friends; 3) Sports Boosters establish a Facebook page to share information about scheduling, wins/losses and support for the team.

Not allowed: A District employee posts a request on a personal Facebook page asking parents to remember to sign their students' permission form for a class activity such a post would be acceptable on a professional "Fan Page," not on a personal page.

Primary (K-5):

For the K-5 level, District employees may use and display social networking and media sites along with their content as part of the District curriculum delivery if the entirety of the material available and viewable

on the site is age appropriate and the focus of the site is educational in nature. Sites that have a primary focus on social interaction and personal content are not allowed for this level.

Example: A teacher accesses an educational web site where the entire content of this site is age appropriate and educational based (TeacherTube). The teacher plays a video excerpt of the education content that applies to the curriculum she is delivering for the class to view directly from the selected web site.

If a K-5 District employee wishes to use content in the classroom from a social networking and media site where the entirety of the content published on the site is not age appropriate, and the focus of the web site is not only educational then that content must be extracted from the site and presented in a neutral format which does not expose the site to the audience.

Example: A teacher locates a video excerpt he or she would like to use as part of his curriculum delivery but it is on a web site that is not specifically focused on education, (YouTube), contains content that is not age appropriate and/or is not related to the educational process. The teacher then downloads the video excerpt and embeds the suitable material into a Microsoft PowerPoint presentation for the class to view without exposing the class to the originating web site.

Additionally, students in the K-5 level should not be given approval by District employees to use social media or networking technologies for student-generated educational content or applications. The same guideline on the use of web-accessed materials that applies to teachers also applies to the student. The material must be extracted from the original site location.

Example: A third grade student is creating a report on lizards. The student finds a video at home on lizards on a web site such as YouTube and wants to show the video to the class. The video excerpt must be extracted from the web site in order to be shown to the class without exposing the originating web site

District Volunteers should not use social media or social networking to communicate with students at the K-5 level.

Secondary (6-12):

For the 6-12 level, District employees may use and display social networking and media sites along with their content as part of the District curriculum delivery as long as the District staff member exercises the utmost due diligence to ensure that content is age appropriate and educational in nature and the entire content that will be displayed and made visible to students is appropriate. (This includes any web page side banners, advertisements, etc. that would be viewable along with the intended educational content.). The use of Social Networking and media is not recommended for individual communications between District employees and students, or between District Volunteers and students.

Example: 1) High school college counselors set up a Twitter feed to make students aware of application deadlines and new opportunities on a more real time basis; 2) Videos from YouTube that are directly

related to the educational subject matter are used from their original site in the classroom using care to ensure that inappropriate content is not visible on the page being viewed; 3) A business teacher has each student develop a LinkedIn account and begin building a professional network within their field of interest; 4) A teacher locates a video on a web site that they would like to use in teaching the lesson plan. The video appears on a site that also has advertisements that are not age-appropriate, rapidly changing and would be viewable by students. The teacher extracts the video to a neutral presentational format for use in the classroom; 5) A student newspaper group wishes to create a web presence to post their student newspaper for consumption by the general public. (This example would require District approval prior to proceeding.)

Text Messaging – Many students in our District have a cell phone, and the use of text messaging is rising sharply. This form of communication is typically between individuals and is virtually instantaneous. District 129 does not currently endorse this technology as a learning tool and requires all student cell phones be silenced and stored out of sight during the academic day. In some circumstances and at certain time frames, text messaging between District employees, District volunteers and students may be allowed such as coordinating communication around extracurricular activities, schedule and venue changes as outlined. For all such texting scenarios, District employees and District volunteers should be aware that text messaging may easily be misinterpreted, making it essential that communications by this method should be crisp, clear and contain appropriate content, and only to students whose parents/guardians have not signed the Permissions Denial form.

District Employees, District Volunteers, Parent/Guardians, General Public: It is preferred that these groups use District email, Voice communications or District Standard applications to communicate District-related business. However, texting is also an approved method to communicate provided that there is foreknowledge, understanding and appropriate contact information exchanged between communications originators and receivers prior to texting occurring.

Example: 1) A parent and a teacher have exchanged phone numbers in order to use texting to communicate electronically. The parent texts the teacher to request a response related to a student lab project; 2) A teacher texts her principal with updates related to a student group presentation at an upcoming assembly; 3) A member of the District administration texts a vendor requesting a delivery date on supplies; 4) A basketball coach texts the parents/guardians of her team members that the bus will be arriving at a specific time after an away game.

Primary (K-5):

District employees or District Volunteers are not allowed to initiate texting or engage in a texting interchange to students at these levels

Example: 1) A student sends a text to her parent after school hours informing the parent that basketball practice will run ½ hour later than expected; 2) A District volunteer texts several parents of K-5 students to coordinate an event; 3) A K-5 student initiates a text conversation with a teacher regarding a homework question. The teacher responds saying he will send an email to or call the parent/guardian

ending the texting interchange; 4) A K-5 student sends a personal text message ("Hi") to a teacher. The teacher disregards the message and does not respond.

Not approved: A District employee asks a K-5 student to send a text message to others on his behalf regarding District-related communication.

Secondary (6-12):

Texting between District Employees or District Volunteers and students at these levels is acceptable provided that student's parents have not signed the Permissions Denial form. Situations such as coaches needing to inform team members of schedule or venue changes, club leadership disseminating information to members etc., fall under this category. However, texting between District employees or District volunteers and students should not be used as a routine or standard form of communications. Texting between District Employees and students should always be strictly regarding District Business. Under no circumstances should text messages between students and teachers be of a personal or non-business related nature.

Example: 1) A chess team leader who is a District employee uses texting with team members and their parents to communicate team related information only; 2) A football coach uses texting to notify a player that they will be starting the next game due to an injury to another player.

Not approved: A teacher invites students to text questions about an assignment if they are having problems as a routine way of addressing student's questions, regardless of the student's parents signing a Permissions Denial form. 2) A teacher sends a mass text to students reminding them of an upcoming text without ensuring that the student's parents have not signed the Permissions Denial form.

Non-District Email Accounts – Any individual with a District-provided email account should not use a personal email account to communicate District business that is subject to FOIA requests and/or contains confidential information about a student or a parent/guardian. It is expected and appropriate that these individuals may receive emails to their District-provided account from any non-District originator using a non-District email account (Gmail, Yahoo, and MSN).

Example: A parent, who is also the teacher's friend, sends an email to the teacher's personal email address concerning a student-related issue. The teacher responds to the email using the District provided email account.

Not allowed: A District employee working from home uses their non-District email account to send copies of meeting minutes to other District employees.

Confidentiality, Privacy, & Student Safety

Unless authorized by the District to do so, District employees, and District volunteers should not post or allow to be posted, confidential student or employee information online or in any electronic format. If you have a question about the confidential status of information, contact your building administrator.

District employees should monitor the networking tools you are providing. Managing social media sites is much like monitoring behavior in a classroom. The posting of content should be structured and monitored to ensure appropriateness of content.

It is recommended that District employees and District volunteers use the highest level of available privacy tools to appropriately control access on sites used professionally, for instruction, and for personal use. Keep in mind that social media sites can change their privacy policies and standards at any time, putting posts you thought were private in the public domain.

Important Reminders for District employees who use Facebook, Twitter, or other Social Media Sites for Personal Purposes

District employees who are presently, or might in the future consider using Facebook or other social media to communicate with friends, family, and their personal networks for Non-District related communications should take care to ensure that their privacy settings are set to "Only Friends." If the "Friends of Friends" or "Networks and Friends" settings are used, employee members open their content to a much larger group of people, including students and parents. While the District employee may never post questionable content, there are no guarantees that one of the District employee's friends will not. District employees should never "friend" students who are currently enrolled in District 129 (or under the age of 18) to your personal account(s), nor should you accept their "friend requests."[1] The boundaries between the role of a public District employee and personal relationships with students should always be upheld and strongly communicated.

As a reminder, District employees, by virtue of their position in the community, are public figures and are personally responsible for content they publish, pictures they post, or dialogue they maintain, regardless of the medium, for the life of the content. No posting by a District employee should compromise the professionalism, integrity, and ethics in their role as an Aurora West School District 129 professional. Before posting content, employees should ask themselves: "Would I mind if that information/image appeared on the front page of the local newspaper?" If the answer is "yes" or "probably," it should not be posted. Contrary to what many people think, email, social media and social networking sites are very public places.

Disclaimer for Personal Postings

Unless conducting District business and authorized by the District to do so, a District employee who identifies themselves as a District employee in content published to any website that is not a District-sponsored site, is requested to use the following disclaimer: "The postings on this site are my own and do not necessarily represent Aurora West School District 129 policy, strategy, or opinion." The disclaimer in itself does not exempt employee from personal and professional responsibility. [2]

Respect all applicable copyright, fair use, and disclosure laws. It is expected that employees of District 129 will not make or post disparaging, discriminatory, defamatory, confidential, threatening, libelous, obscene or slanderous comments about District employees, students, or parents. Do not use Aurora West

School District 129 logos, or school logos, or other District branding on personal social media sites without first obtaining permission from the District Community Relations Director.

[1] District Staff members may "friend" or communicate with personal social media tools with family members who are also students in the district.

[2] This applies to specific posts only. District employees are not required to disclaim their employment on all subsequent posts if they do not identify themselves as district employees in the subsequent post.

5-125 Policy Attachments General Do's and Don'ts.pdf (207 KB)

Book	District Policies
Section	6: Instruction
Title	Administrative Procedure - Acceptable Use of Electronic Networks
Number	6.235 AP
Status	Active
Legal	No Child Left Behind Act, 20 U.S.C. §6777. Children's Internet Protection Act, 47 U.S.C. §254(h) and (l). Enhances Education Through Technology Act of 2001, 20 U.S.C §6751 et seq. Harassing and Obscene Communications Act, 720 ILCS 135/0.01.
Adopted	May, 19, 2014

Safe. Responsible. Respectful.

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. **The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or legal action.**

Terms and Conditions

Acceptable Use - Access to the District's electronic network must be: (a) for the purpose of education or research, and be consistent with the District's educational objectives, or (b) for legitimate business use.

Privileges - The use of the District's electronic network is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator or Building Principal will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. His or her decision is final.

Unacceptable Use - The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law;

b. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;

c. Downloading of copyrighted material for other than personal use;

d. Using the network for private financial or commercial gain;

e. Wastefully using resources, such as file space;

f. Hacking or gaining unauthorized access to files, resources, or entities;

g. Invading the privacy of individuals, that includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature including a photograph;

h. Using another user's account or password;

i. Posting material authored or created by another without his/her consent;

j. Posting anonymous messages;

k. Using the network for commercial or private advertising;

l. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and

m. Using the network while access privileges are suspended or revoked.

Network Etiquette - The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

a. Be polite. Do not become abusive in messages to others.

b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.

c. Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.

d. Recognize that email is not private. People who operate the system have access to all email. Messages relating to or in support of illegal activities may be reported to the authorities.

e. Do not use the network in any way that would disrupt its use by other users.

f. Consider all communications and information accessible via the network to be private property.

No Warranties - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification - The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of these procedures.

Security - Network security is a high priority. If the user can identify a security problem on the Internet, the user must notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

Telephone Charges - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

Copyright Web Publishing Rules - Copyright law and District policy prohibit the re-publishing of text or graphics found on the web or on District websites or file servers without explicit written permission.

a. For each re-publication (on a website or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the web address of the original source.

b. Students and staff engaged in producing web pages must provide library media specialists with email or hard copy permissions before the web pages are published. Printed evidence of the status of "public domain" documents must be provided.

c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material may not be considered a source of permission.

d. The *fair use* rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

e. Student work may only be published if there is written permission from both the parent/guardian and student.

Use of Email - The District's email system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides email to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.

a. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an email account is strictly prohibited.

b. Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.

c. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet *domain*. This domain is a registered name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the School District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.

d. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.

e. Use of the School District's email system constitutes consent to these regulations.

Internet Safety

Internet access is limited to only those *acceptable uses* as detailed in these procedures. Internet safety is almost assured if users will not engage in *unacceptable uses*, as detailed in these procedures, and otherwise follow these procedures.

Staff members shall supervise students while students are using District Internet access to ensure that the students abide by the *Terms and Conditions* for Internet access contained in these procedures.

Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.

The system administrator and Building Principals shall monitor student Internet access.