Electronic Technologies Acceptable Use

I. PURPOSE

The purpose of this procedure is to set forth parameters and guidelines for access to all electronic technologies housed in, operated by or associated in any way with Township High School District 211.

The District's electronic networks and technology, including the Internet, are a part of the District's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation and communication. These guidelines apply to the use of the District's electronic networks and technology for both District-issued electronic devices and personal electronic devices owned by students or staff members.

Employees are expected to use technology that is necessary to perform the duties of their position. Employees who fail to adhere to District policy or administrative procedures are subject to disciplinary action in accordance with their collective bargaining agreement or contract. Disciplinary action may include suspension or withdrawal of Internet or email access, payment for damages or repair, termination and referral to civil or criminal authorities for prosecution.

II. GENERAL STATEMENT OF PROCEDURE

In making decisions regarding employee and student access to the District's computer network, electronic technologies and Internet, the District considers its own educational mission, goals and strategic direction. Access to the District's computer network and Internet enables students and employees to explore libraries, databases, web pages, other online resources, and exchange information and communicate with people around the world. The District expects its instructional staff to blend thoughtful use of the District's computer network, educational technologies and the Internet throughout the curriculum to improve instruction and learning, and to provide exemplary guidance to students about responsible digital citizenship.

III. EDUCATIONAL PURPOSES

The District provides access to the District's electronic technologies to students and employees for specific educational purposes. Students and employees are expected to use electronic technologies to further the District's educational mission, goals and strategic direction. Students and employees are expected to use the District's electronic technologies to support classroom activities, educational research or professional enrichment and effectiveness.

Use of the District's electronic technologies is a privilege, not a right. Misuse of the District's electronic technologies may lead to discipline of the offending employee or student. The District's network, an educational technology, is a limited forum; the District may restrict participation for educational or safety reasons.

IV. GUIDELINES IN USE OF ELECTRONIC TECHNOLOGIES

A. Electronic technologies are assets of the District and are protected from unauthorized access, modification, destruction or disclosure.

B. The District reserves the right to monitor, read or copy any item on or connected to the use of the District's electronic technologies, including its network.

C. Students and employees will not vandalize, damage, disable or hack into any electronic technology or system used by the District.

D. By authorizing use of the District's electronic system or devices, including the electronic network, the District does not relinquish control over materials on, or connected to, the system or contained in files on the system or District-owned or operated devices. Users should not expect privacy in the contents of personal files on the District system.

E. Routine periodic maintenance and monitoring of electronic technologies, including the District network, may lead to a discovery that a user has violated this procedure, another school District procedure, or policy or the law.

V. UNACCEPTABLE USES OF ELECTRONIC TECHNOLOGIES AND DISTRICT NETWORK

The following uses of the electronic technologies and District network ("electronic technologies") are considered unacceptable:

A. Users will not use the District's electronic technologies to access, review, upload, download, complete, store, print, post, receive, transmit or distribute:
   1. Pornographic, obscene or sexually explicit material or other visual depictions;
   2. Obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful or sexually explicit language;
   3. Materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;
   4. Materials that use language or images that advocate violence or discrimination toward other people or that may constitute harassment, discrimination or that threatens the safety of others;
   5. Orders for personal shopping not associated with the work of the District that are placed online during time designated as work time by the District;
   6. Storage of personal photos, videos, music or files not related to educational purposes for any length of time during designated work times;
   7. Any image, message, photo, file or other electronic content that may violate District policy or procedure.

B. Users will not use the District's technologies to create, access, upload, download, post, receive, transmit or distribute any form of audio- or video-recording of students or staff members, or the public distribution of any such recording, without the full, knowledgeable consent of the individual being recorded.

C. Users will not use the District's electronic technologies to knowingly or recklessly create, post, transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

D. Users will not use the District's electronic technologies to engage in any illegal act or violate any local, state or federal laws.

E. Users will not use the District's electronic technologies for political campaigning.

F. Users will not use the District's electronic technologies to vandalize, damage or disable the property of another person or organization. Users will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses, engaging in "spamming" or by any other means. Users will not tamper with, modify or change the District system software, hardware or wiring, or take any action to violate the District's security system. Users will not use the District's electronic technologies in such a way as to disrupt the use of the system by other users.

G. Users will not use the District's electronic technologies to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person.

H. Users must not deliberately or knowingly delete or modify a student or employee file without the owner's permission.

I. Users will not use the District's electronic technologies to post information in public access areas regarding private or confidential information about another person. Private or confidential information is defined by Board policy, state law and federal law.
   1. This paragraph does not prohibit the posting of information to contact an employee using District-issued resources, such as a work phone number or email address.
   2. This paragraph does not prohibit communications between employees and other individuals when such communications are made for legitimate education reasons or personnel-related purposes (i.e., communications with parents or other staff members related to students).
   3. This paragraph specifically prohibits the use of the District's electronic technologies to post private or confidential information about another individual, employee or student on social networks.

J. Users will not attempt to gain unauthorized access to the District's electronic technologies or any other system through the District's electronic technologies, attempt to log in through another person's account or use computer accounts, access codes or network identification other than those assigned to the user. Users must keep all account information and passwords private.

K. Messages and records on the District's electronic technologies may not be encrypted without the permission of the District's chief technology officer.

L. Users will not use the District's electronic technologies to violate copyright laws or usage licensing agreements:
   1. Users will not use another person's property without the person's prior approval or proper citation;
   2. Users will not download, copy or exchange pirated software, including freeware and shareware; and
   3. Users will not plagiarize works found on the Internet or other information resources.

M. Users will not use the District's electronic technologies for unauthorized commercial purposes or financial gain unrelated to the District's mission. Users will not use the District's electronic technologies to offer or provide goods or services, or for product placement.

VI. SOCIAL MEDIA

A. The use of social media to communicate with students provides employees with unique advantages not available in the past. Social media can also lead to miscommunication between students and staff if used incorrectly. The District has an approved school board policy surrounding the use of social media and other forms of electronic communication. The Board of Education policy and the accompanying social media guidelines provide a means to help protect teachers and students in the responsible use of social media.

B. The general rules for communication with social media are:
   1. Be transparent and make certain information and access readily available;
   2. Be professional and for legitimate educational or extracurricular reasons;
   3. Follow all local, state and national guidelines, including the Child Internet Protection Act (CIPA) and all copyright laws;
   4. It should NOT include private or confidential information about other students.

C. Recommended guidelines for using social media can be found in the District 211 Social Media and Electronics Communication Policy. Refer to School Board Policy GBAD for more information.

VII. GUEST ACCESS AND INTERNET USE

A. Guest access to the District's open wireless network is provided as a service to the community and is subject to all policies and guidelines covered in Sections II through V and XIII of this Acceptable Use Agreement, plus any state and federal laws related to Internet use, including copyright laws.

B. Guest access provides filtered, limited bandwidth for our guests to allow access to the Internet, email and VPN services.

C. Limited technical support is provided for guest access and is identified in the service level agreement found on the District technology website.

VIII. EMPLOYEES

A. Use of Email
   1. The District provides access to electronic mail to District employees for the purpose of conducting District-related work and communication.
   2. The email system will not be used for outside business ventures or other activities that conflict with Board policy.
   3. All emails received by, sent through or generated by computers using the District network are subject to review by the District.
   4. Appropriate language must be used when communicating using the District email system or network.
   5. All information contained in an email must be treated in accordance with state and federal laws.
   6. Employees will not provide access to their email accounts to non-employees.
   7. It is recommended that electronic mail contain a confidentiality notice, similar to the following: *"If the information in this email relates to an individual or student, it may be private data under state or federal privacy laws. This individual private data should not be reviewed, distributed or copied by any person other than the intended recipient(s), unless otherwise permitted under law. If you are not the intended recipient, any further review, dissemination, distribution or copying of this electronic communication or any attachment is strictly prohibited. If you have received an electronic communication in error, you should immediately return it to the sender and delete it from your system. Thank you for your compliance"*

B. District Electronic Technologies
   1. The District's electronic technologies are provided primarily for work-related, educational purposes.
   2. Incidental use of the District's electronic network and technologies for personal use, such as checking personal email correspondence or web pages is permitted, but only to the extent that such use does not occur during instructional time, does not interfere with instruction or District operations, and does not violate any law or District policy or procedure. Those who use the District's Electronic Network and Technology for personal use do not have any expectation of privacy to materials accessed therein.

C. Inappropriate use of the District's electronic technologies includes, but is not limited to:
   1. Posting, viewing, downloading, creating or otherwise receiving or transmitting offensive, defamatory, pornographic or sexually explicit materials;
   2. Posting, viewing, downloading, creating or otherwise receiving or transmitting materials that use language or images that advocate violence or discrimination toward other persons;

3. Posting, viewing, downloading, creating or otherwise receiving or transmitting material that may constitute harassment or discrimination contrary to District policy and state and federal law;
4. Engaging in computer hacking or other related activities;
5. Attempting to disable, actually disabling or compromising the security of information contained on the District network or any computer;
6. Engaging in any act that violates any District policy; and
7. Engaging in any illegal act in violation of any local, state or federal laws.

D. Employees may participate in public Internet discussion groups using the District's electronic technologies, but only to the extent that the participation:
   1. Is work-related;
   2. Does not reflect adversely on the District or disrupt the educational environment in any way;
   3. Is consistent with District policy; and
   4. Does not express any position that is, or may be interpreted as, inconsistent with the District's mission, goal or strategic plan.

E. Employees may not use proxy servers to access online content blocked by District filters.

F. Employees may not use the District network or electronic technologies to post unauthorized or inappropriate personal information about another individual on social networks.

G. Employees will observe all copyright laws. Information posted, viewed or downloaded from the Internet may be protected by copyright. Employees may reproduce copyrighted materials only with express permission of the author or publisher.

H. All files downloaded from the Internet must be checked for possible computer viruses. The District's authorized virus-checking software installed on each District computer will ordinarily perform this check automatically; however, employees should contact the District's chief technology officer before downloading any materials for which the employee has questions.

I. Employee Responsibilities
   1. Employees who are transferring positions or leaving positions must leave all work-related files and electronic technologies -- including form letters, handbooks, databases, procedures and manuals, regardless of authorship -- for their replacements.
   2. Individual passwords for computers are confidential and must not be shared.
   3. If an employee's password is learned by another employee, the password should be changed immediately.
   4. An employee is responsible for all activity performed using the employee's password.
   5. No employee should attempt to gain access to another employee's documents without prior express authorization.
   6. An active device with access to private data must not be left unattended and must be protected by password-protected screen savers.

IX. DISTRICT WEB PRESENCE

The District website was established to provide a learning experience for employees and students, and to provide a venue for communications with parents and the community.

A. District Website
   1. The District will establish and maintain a website. The website will include information regarding the District, its schools, District curriculum, extracurricular activities and community education.

2. The District webmaster will be responsible for maintaining the District website and monitoring District web activity.
3. All website content will support and promote the District's mission, goals and strategic direction.
4. The District's website will provide parents with a web portal to classroom- related calendars, grades, attendance, assignments and resources.

B. School Website
1. Each school will establish and maintain a website. The website will include information regarding the school, its employees and activities.
2. The Principal will authorize individuals who will provide content to the webmaster who will be responsible for maintaining the school's website.
3. All website content will support and promote the District's mission, goals and strategic direction.
4. Each school's website will provide parents with a web portal to classroom- related calendars, grades, attendance, assignments and resources.

C. Classroom and Teacher Web Pages
1. The District encourages all teachers to establish a web page that supports their classroom instruction.
2. If a teacher establishes a web page, he or she is responsible for maintaining the web page.
3. All classroom and teacher web pages must be linked to a school website.

D. Student Web Pages
1. Students may create web pages as part of classroom activities with teacher supervision.
2. Student web pages must include the following notice: "This is a student- produced web page. Opinions expressed on this page are not attributable to the District."
3. For all classroom-related projects posted to the Internet, the content must abide by all District 211 policies. Rules that apply to the classroom also apply to assignments and communication that are posted online.
4. The classroom teacher will review student-produced web pages to determine if the contents should be removed at the conclusion of the course or grading period.

E. Department and Non-Instructional Web Pages
1. Departments and non-instructional programs may also create web pages to support their departments or programs.
2. The establishment of web pages must be approved by the District webmaster.
3. Once established, the individual departments or programs must appoint a webmaster who will maintain the web page.

F. Extracurricular Web Pages
1. With the approval of the building principal and District webmaster, a School-Board-sanctioned extracurricular organization may establish a web page.
2. All web page content will support the extracurricular organization and the District's mission, goals and strategic direction.
3. The building principal and District webmaster will oversee the content of these web pages.
4. School-Board-sanctioned extracurricular organizations' web pages must include the following notice: *"This is an organization-produced web page. Opinions expressed on this page are not attributable to the District."*

X. CYBER-BULLYING

A. Cyber-bullying is the use of electronic information and communication devices to willfully harm either a person or persons through the medium of electronic text, photos or videos.

B. Employees are not permitted to create, post or transfer any discriminatory, confidential, threatening, libelous, obscene or slanderous comments about District 211, its employees, students, parents, School Board members or community members.

C. Cyber-bullying creates a hostile, disruptive environment on the school campus and is a violation of a student's or employee's right to be safe and secure. It is a serious offense that will lead to disciplinary action.

XI. INFORMATION PROVIDED TO STUDENTS

A. The proper use of the Internet and educational technologies, and the educational value to be gained from proper usage is the joint responsibility of students, parents and employees of the District.

B. Students have access to Internet resources through the District's wireless network, classrooms, the media centers, District-provided electronic devices, personal electronic devices and school computer labs. Access to the District's wireless network can be found throughout each school and while on the school campus outside the school building.

C. Students using social networking tools and curriculum content management software for a teacher's assignment are required to keep personal information, as stated above, out of their postings.

D. Parents' Responsibility
Outside of school, parents bear responsibility for the same guidance of Internet use as they exercise with other technology information sources. Parents are responsible for monitoring their student's use of the District system and District educational technologies if the student is accessing the District system from home or a remote location, or if the student is using a District-provided device.