Buffalo Independent School District

708 Cedar Creek Road
Buffalo, Texas 75831
Phone: (903) 322-3765 Fax: (903) 322-3091
Lacy G. Freeman, Superintendent

Electronic Technologies Acceptable Use

I. Purpose

The purpose of this policy is to set forth policies, parameters and guidelines for access to the district's electronic technologies, including electronic communications, the district's network and Internet social networking tools. The school district will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

II. General Statement of Policy

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 messages 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, providing guidance to students.

III. Educational Purposes

The district purpose in offering access to the district's electronic technologies to students and employees is more specific than providing them with general access. Use of the district's electronic technologies is for a limited educational purpose.

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.

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 speech for educational 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 using the district's electronic technologies, including its network.

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

D. By authorizing use of the district system, the district does not relinquish control over materials on the system or contained in files on the system. Users should not expect privacy in the contents of personal files on the district system.

E. Routine maintenance and monitoring of electronic technologies, including the district network, may lead to a discovery that a user has violated this policy, another school district 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 threatens the safety of others;
5. Orders for shopping 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.

B. Users will not use the district's electronic technologies to knowingly or recklessly 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.

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

D. Users will not use the district's electronic technologies for political campaigning.

E. 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.

F. 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.

G. Users must not deliberately or knowingly delete a student or employee file.

H. 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 employee contact information on district web pages.
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 the district's electronic technologies to post private or confidential information about another individual, employee or student, on social networks.

I. Users will not repost or resend a message that was sent to the user privately without the permission of the person who sent the message.

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 director technology services.

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. User Notification

Users will be notified of the district policies relating to Internet use. This notification must include the following:

A. Notification that Internet use is subject to compliance with district policies.

B. Disclaimers limiting the district's liability relative to:
1. Information stored on district disks, drives or servers.
2. Information retrieved through district computers, networks or online resources.
3. Personal property used to access district computers, networks or online resources.
4. Unauthorized financial obligations resulting from use of district resources or accounts to access the Internet.

C. A description of the privacy rights and limitations of district sponsored or managed Internet accounts.

D. Notification that the collection, creation, reception, maintenance and dissemination of data via the Internet, including electronic communications, is governed by district, state and federal policies.

E. Notification that should the user violate the district's acceptable use policy, the user's access privileges may be revoked, academic sanctions may result, school disciplinary action may be taken, and/or appropriate legal action may be taken.

F. Notification that all provisions of the acceptable use policy are subordinate to local, state and federal laws.

G. Family Notification
1. Notification that the district shall use technical means to limit student Internet access, however the limits do not provide a foolproof means for

enforcing the provisions of this acceptable use policy.

2. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student or the student's parents.

VII. Students

A. Internet Use Agreement

1. 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.

2. This policy requires the permission of and supervision by the school's designated professional staff before a student may use a district account or educational technologies to access the Internet.

3. The Internet use agreement form (see Appendix I) for students must be read and signed by the student and the parent or guardian. The agreement must be signed in order to be granted access to the Internet via the district network. This policy requires that the signed, up-to-date form be retained electronically or physically.

4. A signature is required when the student begins in the district, in 3rd grade, in 4th grade and in 9th grade.

5. Students have access to Internet resources through their classroom, library or school computer lab.

6. 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 (see Section V.H).

7. Students using the district's educational technologies for social networking for a limited educational purpose must follow the Buffalo ISD policy on bullying.

B. Parents' Responsibility; Notification of Student Internet Use

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.

VIII. 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 policy, plus any state and federal laws related to Internet use, including copyright laws.

B. Guest access provides limited bandwidth, filtered for the following services:

1. Web access (http and https)
2. Email services (pop, imap)

IX. Employees

A. Use of Email

The district provides access to electronic mail for business communication between district employees and its customers.

1. The email system will not be used for outside business ventures or other activities that conflict with board policy.

2. All emails received by, sent through, or generated by computers using the district network are subject to review by the district.

3. Appropriate language must be used when communicating using the district email system or network.

4. All information contained in an email must be treated in accordance with district, state, and federal policies regarding student and employee data privacy.

5. Employees will not provide access to their email accounts to non-employees.

6. It is recommended that electronic mail must 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. Inappropriate use of the district's electronic technologies includes, but is not limited to:

a. Posting, viewing, downloading or otherwise receiving or transmitting offensive, defamatory, pornographic or sexually explicit materials;
b. Posting, viewing, downloading or otherwise receiving or transmitting materials that use language or images that advocate violence or discrimination toward other persons;
c. Posting, viewing, downloading or otherwise receiving or transmitting material that may constitute harassment or discrimination contrary to district policy and state and federal law;
d. Engaging in computer hacking or other related activities;
e. Attempting to, actually disabling or compromising the security of information contained on the district network or any computer; and
f. Engaging in any illegal act in violation of any local, state or federal laws.

3. Employees may participate in public Internet discussion groups using the district electronic technologies, but only to the extent that the participation:

a. Is work-related;
b. Does not reflect adversely on the district;
c. Is consistent with district policy; and
d. Does not express any position that is, or may be interpreted as, inconsistent with the district's mission, goal or strategic plan.

4. Employees may not use proxy servers to access online content blocked by district filters.

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

6. 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 in accordance with district, state, and federal policy.

7. All files downloaded from the Internet must be checked for possible computer viruses. The district authorized virus checking software installed on each district computer will ordinarily perform this check automatically; however, employees should contact the district's director of media and technology services before downloading any materials for which the

employee has questions.

C. 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.

a. If an employee's password is learned by another employee, the password should be changed immediately.
b. An employee is responsible for all activity performed using the employee's password.
c. No employee should attempt to gain access to another employee's documents with prior express authorization.
d. An active terminal with access to private data must not be left unattended and must be protected by password protected screen savers.

3. Employees are expected to use technology necessary to perform the duties of their position.

4. Employees who fail to adhere to district policy 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.

X. 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 appoint a 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. The classroom teacher and school webmaster will approve all student produced web content prior to its posting.

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 Noninstructional Web Pages

1. Departments and noninstructional 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 schoolboard 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."

XI. Records Management and Archiving

All technological data is data under the Family Educational Rights and Privacy Act, Records Retention Schedule, and school board policy.

XII. Filter

A. With respect to any of its computers with Internet access, the district will follow the guidelines provided by the Children's Internet Protection Act, and will monitor the online activities of users and employ technology protection measures during any use of such computers by users. The technology protection measures utilized will block or filter Internet access to any visual depictions that are:

1. Obscene;
2. Child pornography; or
3. Harmful to minors.

B. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion; or
2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts or a lewd exhibition of the genitals; and
3. Taken as a whole, lacks serious literary, artistic, political or scientific value as to minors.

C. An administrator, supervisor or other person authorized by the superintendent may modify the technology protection measure, during use by an adult employee, to enable access for bona fide research or other lawful purposes.

XIII. Liability

Use of the district's educational technologies is at the user's own risk. The system is provided on an "as is, as available" basis. The district will not be responsible for any damage users may suffer. The district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system, nor is it responsible for damages or injuries from improper communications or damage to property used to access school computers and online resources. The district will not be responsible for financial obligations arising through unauthorized use of the district's educational technologies or the Internet.

XIV. Implementation; Policy Review

A. The district administration may develop appropriate user notification forms, guidelines and procedures necessary to implement this policy for submission to the school board for approval. Upon approval by the school board, such guidelines, forms and procedures will be an addendum to this policy.

B. The administration will revise the user notifications, including student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.

C. The district educational technologies policy is available for review by parents, employees and members of the community.

D. Due to the rapid evolution in educational technologies, the school board will conduct an annual review of this policy.

Legal References:15 U.S.C. § 6501 *et seq.* (Children's Online Privacy Protection Act) 17 U.S.C. § 101 *et seq.* (Copyrights) 20 U.S.C. § 6751 *et seq.* (Enhancing Education Through Technology Act of 2001) 47 U.S.C. § 254 (Children's Internet Protection Act) 47 C.F.R. § 54.520 (FCC rules implementing CIPA)

Appendix I

STUDENT ONLINE ACCEPTABLE USE CONSENT FORM

Student

By signing below, I agree to follow Buffalo ISD's Electronic Technologies Acceptable Use policy. I understand that my use of the network is a privilege and requires proper online etiquette. I further understand that misuse of the network will result in disciplinary action.

Student Name (PRINT)_____

Student's I.D. Number_____
(MIDDLE SCHOOLS AND HIGH SCHOOL ONLY)

Student's Signature_____
(MIDDLE SCHOOLS AND HIGH SCHOOL ONLY)

Address Zip_____

Telephone Number_____

School Building_____

Parent or Guardian

I give permission for my child to have access to the Internet using the district's computer network. I also understand that some material accessible through the interconnected systems may be inappropriate for school-age students. I agree to defend, indemnify and hold harmless Buffalo ISD from any and all claims arising out of or related to the use of this interconnected computer system. I further understand that I have the right to withdraw my approval in writing at any time.

Approved ☐

Disapproved ☐

Parent/Guardian Name (PRINT)_____

Signature of Parent/Guardian_____

Date_____

Return this form to your school.

Appendix II

ONLINE CODE OF ETHICS

1. Students accessing or using Web 2.0 products including but not limited to blogs, wikis, podcasts, Google applications and Moodle for student assignments are required to keep personal information out of their postings. Students will not post or give out photographs of themselves or others, their family name, password, user name, email address, home address, school name, city, country or other information that could help someone locate or contact them in person.

2. Students will not log in to the network as another classmate.

3. Students using Web 2.0 tools will treat these tools as a classroom space. Speech that is inappropriate for class is not appropriate on Web 2.0 tools. Students are expected to treat others and their ideas online with respect.

4. Assignments on Web 2.0 tools are like any other assignment in school. Students, in the course of completing the assignment, are expected to abide by policies and procedures in the student handbook, including those policies regarding plagiarism and acceptable use of technology.

5. Student blogs are to be a forum for student expression; however, they are first and foremost a tool for learning. The district may restrict speech for valid educational reasons as outlined in board policy.

6. Students shall not use the Internet, in connection with the teacher assignments, to harass, discriminate, bully or threaten the safety of others. If students receive a comment on a blog or other Web 2.0 tool used in school that makes them feel uncomfortable or is not respectful, they must report this to a teacher, and must not respond to the comment.

7. Students accessing Web 2.0 tools from home or school, using school equipment, shall not download or install any software without permission, and not click on ads or competitions.

8. Students should be honest, fair and courageous in gathering, interpreting and expressing information for the benefit of others. Always identify sources and test the accuracy of information from all sources.

9. Students will treat information, sources, subjects, colleagues and information consumers as people deserving of respect. Gathering and expressing information should never cause harm or threaten to be harmful to any person or group of people.

10. Students are accountable to their readers, listeners, viewers and to each other. Admit mistakes and correct them promptly. Expose unethical information and practices of others.

11. School board policies concerning acceptable use of electronic technology include the use of these Web 2.0 tools for school activities (Policy 622 – Copyright Policy and Policy 634 – Electronic Technologies Acceptable Use).

12. Failure to follow this code of ethics will result in academic sanctions and/or disciplinary action.

Appendix III

GUIDELINES FOR EMPLOYEE'S PERSONAL USE OF SOCIAL NETWORKING

The decision to use online social networking for personal use is at the employee's discretion. The district does not affirmatively monitor employee use of nondistrict, online social networking tools if the employee is not using district electronic technologies; however, the district may take appropriate action when it becomes aware of, or suspects, conduct or communication on an online social media site that adversely affects the workplace or violates applicable professional codes of ethics. These guidelines are for employees engaging in social networking for personal use.

1. When using your personal social networking sites, refrain from fraternization with students.
2. Ensure that social networking postings are appropriate for the public.
3. Weigh whether a posting will put your effectiveness as an employee at risk.
4. Use caution with regard to exaggeration, profanity, guesswork, copyrighted materials, legal conclusions and derogatory comments.
5. Ensure compliance with data privacy laws and district policies. Employees will be held responsible for inappropriate disclosure, whether purposeful or inadvertent.
6. Respect your coworkers and students. Do not discuss students, their families or coworkers.
7. Student images obtained from your employment with the district should not be included on personal social networking sites.
8. Set privacy settings carefully to ensure that you know who has access to the content on your social networking sites.
9. If the public may consider your statements to be made in your capacity as a district employee, you may want to include "this posting is my own and does not represent the view of Buffalo ISD." An employee in a leadership role in the district, by virtue of his or her position, must consider whether personal thoughts he or she publishes will be attributed to this district.
10. Social media identifications, login identifications, and user names must not contain the district's name or logo without prior written permission from (1) the director of media and technology and (2) the director of community education services or superintendent's designee.

Appendix IV

GUIDELINES FOR CLASSROOM USE OF SOCIAL MEDIA TOOLS

The district provides teachers with password-protected, online social media tools that can be used for instruction. Teachers may also elect to use other social media tools for the purpose of instruction in accordance with Policy 634 – Electronic Technologies Acceptable Use and its appendices.

A. District Online Social Media Tools

1. Content and use must adhere to district policies and guidelines.
2. The platform for instruction must indicate that views expressed on the social media site are that of the employee or student, and do not necessarily reflect the views of Buffalo ISD.
3. The teacher must not disclose information on any online social media site that is district property, protected by data privacy laws, or in violation of copyright.

B. Nondistrict Social Media Tools

1. If a teacher elects to use a nondistrict social media tool, the teacher must build a separate page in that social media tool from his or her personal online presence.
2. Content and use must adhere to district policies and guidelines.
3. Content and use must not violate the “terms of service” for the social media tool.
4. The platform for instruction must indicate that views expressed on the social media site are that of the employee or student, and do not necessarily reflect the views of Buffalo ISD.
5. The teacher must not disclose information on any online social media site that is district property, protected by data privacy laws, or in violation of copyright.
6. The platform must not use official district or school logos without the permission of (1) the director of community education services or superintendent’s designee and (2) the director of media and technology.

Appendix V

GUIDELINES FOR SCHOOL OR DISTRICT USE OF SOCIAL MEDIA TOOLS

Individual schools and departments may choose to establish an official presence on public online social media sites with prior administrative approval. A request must contain the following information:

1. Sponsoring school or department;
2. Proposed social media site or other location;
3. Purpose of site, which cannot be served by the current district website;
4. Plan on how to comply with district policies and record retention requirements;
5. Description and primary use of site; and
6. Plan for monitoring site, addressing policy violations, and ensuring current content.

The request should be submitted to the director of media and technology. Written approval or denial will be provided to the school or department. If the request is denied, the school or department may request reasons for the denial in writing.

If the request is approved, the school must submit to the director of media and technology, within two weeks of developing the site, the name of the person(s) who will manage the site and the login information for the site. When a presence is established, the sponsoring school or department is responsible for keeping the site current and monitoring the content of the site.

Sites may be linked from the official district website. All sites must comply with web publishing guidelines found in the Electronic Technologies Acceptable Use and record retention requirements.

Appendix VI

Buffalo Independent School District

Electronic Technologies Acceptable Use Policy Receipt

I, _____, have received and read the Buffalo ISD Electronic Technologies Acceptable Use Policy and agree to follow the guidelines and procedures outlined. I further understand that failure to comply with all faculty expectations and responsibilities will be reflected in my evaluation and may result in the implementation of a growth plan or loss of employment.

_____

Signature

_____

Date