INSTRUCTION

Rules and Regulations - Computer Network, Internet Safety, and Technology, Access, and Use

I. Authorization for Computer Network Access

A. Scope of Rules and Regulations and School District Authority

These Rules and Regulations are promulgated pursuant to the Computer Network, Internet Safety, Technology Access, and Use Policy (the "Policy"). These Rules and Regulations govern all use of District technology, the District's local and/or wide area network, and access to the Internet through District computers or the District's local and/or wide area network, which will be collectively referred to in these Rules and Regulations as the District's "technology."

The rights of the District include, but are not limited to, those set forth in the Policy and these Rules and Regulations. The Policy and these Rules and Regulations may be supplemented by additional rules, regulations, and other terms and conditions of technology use that may be promulgated by the Superintendent or his or her designee(s) pursuant to the Policy or these Rules and Regulations.

B. Philosophy of Computer Network Use

The goal of the District 106 Board is to include appropriate computer network access in the District's instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication. All use of the District 106 technology shall conform to the requirements of all District 106 policies. Access to the Internet through the District 106 technology must be for the purpose of education or research and must be consistent with the educational objectives of the District.

C. Authorized Users

Authorized users of the technology include teachers, administrators, other employees of the District, and students who have submitted the appropriate authorization(s) for technology access and whose technology privileges are not suspended or revoked.

D. Students

Students must obtain a Computer Network and Technology Access Code prior to accessing the computer network. In order to obtain a Computer Network and Technology Access Code and to use the district technology a student must submit a copy of the Authorization and Agreement to Follow Rules for Technology Access (Attachment A) signed by the student and his or her parent or guardian. All students who submit this authorization will be provided with a Computer Network Access Code and storage space on the school server. Students will not be permitted to access the Internet through the computer network, however, unless the student's parent or guardian has specifically authorized Internet access.

Unless a student's computer network privileges have been suspended or revoked, the Authorization and Agreement and Student Technology Access Code will be valid so long as the student attends the school. If a student's computer network privileges are suspended or revoked, a newly signed copy of the student and parental authorizations must be submitted before the student's access privileges are restored.

Any violation of the terms of this Authorization, of the Policy, of these Rules and Regulations, or of additional rules, regulations, or other terms and conditions of technology access promulgated by the Superintendent or his or her designee(s) will result in the suspension or revocation of technology privileges, disciplinary action, and/or appropriate legal action.

E. Teachers and Other Non-Students

Teachers and all other non-student users must obtain a Computer Network Access Code prior to accessing the computer network. To obtain a Computer Network Access Code, teachers and other non-students must submit a signed copy of the Teacher and Non-Student Authorization for Computer Network and Internet Technology Access (Attachment B).

Unless a teacher's or other non-student's computer network privileges have been suspended or revoked, this authorization and Computer Network Access Code will be valid so long as the user remains an employee of the District. If a teacher's or other non-student's computer network privileges are suspended or revoked, the user must submit a newly-signed non-student authorization before the user's access privileges are restored.

Any violation of the terms of this Authorization, of the Policy, of these Rules and Regulations, or of additional rules, regulations, or other terms or conditions of technology access promulgated by the Superintendent or his or her designee(s) will result in the suspension or revocation of technology privileges, disciplinary action, and/or appropriate legal action.

II. Student Use of Technology

A. Procedures

Students might have access to information that may not be appropriate to the educational setting through access to other networks and people around the world. In hopes of preventing access to inappropriate information, Bannockburn School District 106 does filter the Internet. Students in Kindergarten through fourth grades will not be allowed to search the Internet without direct adult supervision. Specific sites will be selected by teachers. Fifth through eighth grade students will be allowed to do purposeful searches for specific projects with teacher permission and under direct adult supervision.

B. Network Etiquette and Safety

The District's primary concern in maintaining Internet access is that student safety and security not be compromised at any time. A Safety Education Program is provided yearly by the Bannockburn Police Department. Students themselves can only implement some of the most effective safety measures. With respect to the computer network, teachers and parents should discuss technology use with their students. The student is expected to abide by the generally accepted rules of network etiquette and safety. These include, but are not limited to, the following:

1. Students should not give out such personal information as their name, age, address, telephone number, parents' work address or telephone number, or the name and location of the school over the Internet. Students should not give out such personal information about other individuals over the Internet.
2. Students should tell their parents or teacher immediately if they come across any information on the Internet that makes them feel uncomfortable.
3. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
4. Be polite. Do not become abusive in messages to others.

C. Use of Electronic Mail

The Bannockburn School District's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides e-mail to aid students and staff members in fulfilling their duties and responsibilities, and as an educational tool.

1. 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 electronic account is strictly prohibited.
2. Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail that would be inappropriate in a letter or memorandum
3. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet "domain". This domain name is a registered domain 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 help personally responsible for the content of any and all electronic mail messages transmitted to external and internal recipients.
4. 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.
5. Use of the School District's electronic mail system constitutes consent to these regulations.

III. Privacy

All electronic communications or files created on, stored on, or sent to, from, or via the computer network are the property of the District. Consequently, users do not have any expectation of privacy with respect to such messages and files. Users should remember that such messages and files could be recovered from the computer network's back-up system even after they have been deleted from a user's individual account. Messages relating to or in support of illegal activities may be reported to the authorities.

The Superintendent, Building Principal, and/or their designees may access and review such messages and files when necessary to maintain the integrity and efficient operation of the computer network; to monitor compliance with the Policy, these Rules and Regulations, and all other rules, regulations, or other terms or conditions of computer network access promulgated by the Superintendent or his or her designee(s); and to further all other educational, safety, and pedagogical concerns of the District. The District also reserves the right to intercept, access, and disclose to appropriate authorities all information created with, sent to, received by, or stored on the computer network at any time, with or without user notice. Use of the District's computer network to create, store, send, receive, view, or access any electronic communication or other file constitutes consent by the user for the District to access and review such files consistent with this paragraph. E-mail accounts, which are issued by the District to any user, remain the property of the District, and the District reserves the right to disclose the e-mail addresses of accounts issued to teachers and other non-student users to parents and other members of the public consistent with legitimate District purposes.

IV. District Technology Use

A. Acceptable Use

Access to the District technology must be for bona fide educational or research purposes consistent with the District's educational mission. Access also must comply with the Policy, these Rules and Regulations, other rules, regulations or other terms or conditions of computer network access promulgated the Superintendent or his or her designee(s), and all other disciplinary policies and regulations necessary for the safety and pedagogical concerns of the District.

User responsibilities include, but are not limited to the following:

- Users will be responsible for using the technology as an appropriate educational tool.
- Users will respect the privacy of other users. Students should never read or tamper with files or mail of other people, or use the network to disrupt the work of others.
- Users are responsible for following copyright laws.
- Users have the responsibility to help keep all technology in working order.
- Users will immediately notify a teacher or system administrator if they identify a possible hardware, software, or security problem.

- Users will never give out personal information such as last name, home address, or phone number. (The school's address will be used when needed)
- Users are responsible for all material created, sent or received under his/her user account and therefore should not give out their password to anyone.
- Users need to understand that the technology facilitators have access to all user directories, data, email, web pages, and all other files stored on Bannockburn School District servers and computers.
- District staff will gain permission from students and their parents when posting individual student pictures or work on the Internet. (Attachment C)

B. Unacceptable Use

Any use, including off-campus internet misconduct, which disrupts the proper and orderly operation and discipline of the schools in the District; violates the rights of others; is socially inappropriate or inappropriate for a student's age or maturity level; is primarily intended as an immediate solicitation of funds; is illegal or for illegal purposes of any kind; or constitutes gross disobedience or misconduct is an unacceptable use. Use of the District technology for any unacceptable use will result in the suspension or revocation of computer network privileges, disciplinary action, and/or appropriate legal action.

Unacceptable uses of technology include, but are not limited to the following:

- Student use of the Internet for anything that does not have an appropriate educational purpose.
- Using technology to create, send, solicit, or receive materials that contain racist, sexist, obscene, or otherwise objectionable material that would demean, defame, denigrate others for race, religion, creed, color, national origin, ancestry, physical handicap, gender, etc.
- Using technology to threaten other users or any property regardless of whether or not the user intends to carry out the threat.
- Using technology to harass other users or individuals.
- Students sending messages that include personal information about oneself or other people.
- Student checking of personal email that is not school related.
- Students using online messaging services (AIM, Yahoo Messenger, etc.), chat rooms, shopping sites, sport sites and music sites.
- Deliberately accessing, creating, submitting, posting, publishing, sending, soliciting, or receiving material that contains inappropriate language, text, sounds, or images.

- Copying or downloading materials in violation of state and federal copyright laws. (This means unauthorized copying of software or videos, is prohibited. Also using copyrighted materials from software, books, the Internet or videos without receiving permission from the author is prohibited).
- Unauthorized downloading of games and software from the Internet
- Gaining unauthorized access to the system, which includes logging on via another person's account, with or without their permission, accessing student record data, disclosing any personal account information (including your own), receiving or reading other people's messages, or destroying another's work.
- Using the Bannockburn School District's technology for financial gain, for commercial activity or for any illegal activity.
- Intentionally damaging any of the district's technology.
- Posting material authored or created by another without his/her consent.
- Posting anonymous messages.
- Accessing, submitting, electronically posting materials on the web, transmitting material by cell phone that threatens, demeans, or bullies other students, staff members or the school, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material.
- Modifying, disabling, compromising, or otherwise circumventing the District's filter to access any external network or websites that are deemed inappropriate.
- Using the computers while privileges are suspended or revoked.
- Using the Internet when Internet privileges are suspended or revoked.
- Transmitting documents via Bluetooth exchange between computers/laptops without teacher/administrator authorization.
- Using technology to harass other users or individuals which threaten, or which may reasonably be interpreted to threaten, any person, group of persons, building or property with harm, regardless of whether the user intended to carry out such threat.

V. Technology Protection Measures

Consistent with the District's legitimate educational and pedagogical concerns, the District shall implement technology protection measures, which may include filtering and/or blocking software, with respect to every District computer, which has access to the Internet. Such technology protection measures shall be implemented in the best manner practicable to prevent access to any material, including visual depictions, which are obscene; which constitutes pornography, including child pornography; or which, with respect to use of computers by minors, would be harmful to minors. The District may disable the technology protection measure with respect to an individual computer during

use by non-student adults to enable access to material needed for research or other lawful purposes.

The District shall monitor the use of the technology by students and any other minor users in order to ensure compliance with this Technology policy, these rules and regulations, other rules, regulations, or other terms or conditions of technology access publicized by the District, and other disciplinary policies and regulations necessary to further the educational, safety, and pedagogical concerns of the District.

VI. Internet and Television Publishing Guidelines

A. Occasionally student-related information or material created by students or staff may be published on the District website. All publishing will follow the following guidelines:

- No student will be personally identified in any published photograph.
- A student's home address, telephone number, e-mail address, or other information which would allow a website visitor to personally contact the student will not be published on the website.
- Work prepared by a student shall not be published on the District website unless the student has submitted a signed Authorization for *Publication of Student Work on District Website* (Attachment C).
- Any material which is proposed to be published on the District's website must be sponsored by a district employee and approved by the District Administrator.
- Any communication concerning a student's work that has been published on the District's website shall be directed to the sponsoring staff member.
- All material published on the District's website must be appropriate for the District's educational mission. All student and staff works submitted for publication on the District's website are subject to treatment as District-sponsored publications.
- Any other objections to publication of a student's photograph and/or work need to be submitted in writing to the School District.

B. There is also the occasion when students are filmed for numerous events, including but not limited to school assemblies, talent shows, or student projects. The publication of such filming will follow the following guidelines:

- No student's image will be shown on the cable television channels unless the student has submitted the signed Authorization form entitled *Authorization to Release Student's Image to Local Cable Television* (Attachment D).

VII. Student-Created or Distributed Written or Electronic Material Including Blogs

A student engages in gross disobedience and misconduct and may be disciplined for creating and/or distributing written or electronic material, including Internet material and blogs, that causes substantial disruption to school operations or interferes with the rights of other students or staff members.

VIII. Security

The security and integrity of the District's technology is a high priority. Users' Network Log In and passwords are secured and are to be kept confidential at all times. If a user believes at any time that he or she has identified a security gap, weakness, or breach, the user must notify a District Staff member immediately. The user may not exploit the gap, weakness, or breach, and the user may not inform any other individuals of it. Any user who violates this security policy may be subject to a suspension or revocation of technology privileges, disciplinary action, and/or appropriate legal action.

IX. 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, equipment, the Internet, or any other network. This includes, but in not limited to, the uploading or creation of computer viruses.

X. No Warranties

A. The District makes no warranties of any kind for the service of providing technology access to its users and bears no responsibility for the accuracy or quality of information or services obtained from the technology or any loss data suffered in connection with use of the technology. The District will not be responsible for any damages or loss suffered by the user resulting from use of technology. Use of any information obtained via the technology is at the user's own risk. The District denies any responsibility for the accuracy or quality of information obtained.

B. 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 relating to, or arising of, an individual user's use of technology.

C. Although the District has acted in a reasonable manner in selecting and implementing filtering and blocking software, and other technology protection measures to prevent access to materials that are inappropriate, by using the District's technology users acknowledge that such technology measures do not prevent access to all prohibited

material, and may prevent access to non-prohibited material. The District assumes no responsibility for access gained or denied by technology protection measures that have been implemented.

XI. Responsibility for Financial Obligations

Use of the District's computer technology may result in financial obligations, such as costs for goods or services that are ordered over the Internet, or damages that are caused by misuse of the computer technology. Each user (or, in the case of a student user, the user's parent(s) or guardian(s), agrees to accept sole and full responsibility for any financial obligations to the District or to other parties that may arise as a result of his or her own (or his or her child's own) use of the computers or it's technology, including, but not limited to, damage to the district network, computers or laptops, telephone charges, long-distance charges, per-minute surcharges, or equipment or line costs.

XII. Cooperation with Investigations

The District reserves the right to participate and cooperate fully in any investigation requested or undertaken by either law enforcement authorities or a party alleging to have been harmed by use of the technology and computer network. The school has the right to enforce policies and procedures with your child's Internet activity if it has nexus with the school. Evidence of illegal activity or a violation of school policy may be reported or turned over to appropriate authorities.

XIII. Enforcement

The failure of any user to abide by the Policy, these Rules and Regulations, or other rules, regulations, or other terms or conditions of computer network access promulgated by the Superintendent or his or her designee(s) will result in the suspension or revocation of the user's computer network privileges, disciplinary action, and/or appropriate legal action. The Superintendent, Building Principal, or their designees may revoke computer network privileges. Other disciplinary measures, if any, will be considered and imposed consistent with District discipline policies.

XIV. Policy Modifications

The Board of Education or the Superintendent may modify these Rules and Regulations at any time. The Superintendent or his or her designee(s) may also establish such other

rules, regulations, or terms or conditions of technology access as may be necessary to ensure the safe, proper, and efficient operation of the technology and the District school. Notice of any such modifications or additional rules, regulations, or other terms or conditions of access shall be promptly communicated to all authorized users, including by posting such modifications on the computer network or in a conspicuous place at access locations. Use of the computer network constitutes acceptance of the terms of the Policy, these Rules and Regulations, and any additional rules, regulations, or other terms or conditions of computer network access, which may have been promulgated by the Superintendent or his or her designee(s)