Student Acceptable Use Policy for Electronic Networks

Each student and his or her parent(s)/guardian(s) must sign the Student Authorization for Electronic Network Access authorization before being granted access to the District's electronic network. The parent/guardian may revoke this consent at any time by notifying the Building Principal in writing.

Purpose

Whiteside School District 115 provides all students access to computers, networks, and the Internet as a means to enhance their education. It is the intent to promote the use of computers in a manner that is responsible, legal, ethical, and appropriate. The purpose of this policy is to assure that all users recognize the limitations that are imposed on their use of these resources. Electronic networks, 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. All use of the District's electronic network must be: (1) in support of education and/or research, and be in furtherance of the goals stated herein, or (2) for a legitimate school business purpose.

The District is not responsible for any information that may be lost or damaged, or become unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Curriculum

The District's electronic network is part of the curriculum and is not a public forum for general use. The use of the District's electronic networks shall: (1) be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and (2) comply with the selection criteria for instructional materials and library-media center materials.

Authorized Users

The District's electronic network is intended for the use of authorized users only. This also applies to the District's Wi-Fi network. Authorized users include students, staff, and others with a legitimate educational purpose for access as determined by the District. Individual schools may grant guest access on a temporary basis, but only for bona-fide school-related activities. Any person using the network, or using any devices attached to the network, agrees to abide by the terms and conditions set forth in this *Student Acceptable Use Policy for Electronic Networks*.

Assumption of Risk

The District will make a good faith effort to keep the District network system in working order and its available information accurate. However, users acknowledge that there is no warranty or guarantee of any kind, either express or implied, regarding the accuracy, quality, or validity of any of the data or information residing on the District network or available from the Internet. The District has no ability to maintain such information and has no authority over these materials. For example, and without limitation, the District does not warrant that the District network will be error-free or free of computer viruses. In making use of these resources, users agree to release the District from all claims of any kind, including claims for direct or indirect, incidental, or consequential damages of any nature, arising from any use or inability to use the network, and from any claim for negligence in connection with the operation of the District network. Use of District computers and/or the District network is at the risk of the user.

Indemnification

The user indemnifies and holds the District harmless from any claims, including attorney's fees, resulting from the user's activities while utilizing the District network that cause direct or indirect damage to the user or third parties.

Security

Network security is a high priority. If a student inadvertently accesses inappropriate information, he or she should immediately disclose the inadvertent access to a teacher or building principal. If a user can identify a security problem on the network/Internet, he or she must notify a teacher or building principal and must not demonstrate the problem to other users. The teacher or building principal should then report problems to the Technology Department. Keep your account and password confidential. Attempts to logon to the network 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.

Expectations and Use

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

Students have no expectation of privacy in any material that is stored, transmitted, or received via the District's electronic network or District computers. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

General rules for behavior and communications apply when using electronic networks. The District's *Student Acceptable Use Policy for Electronic Networks* does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. **The failure of any user to follow the terms of this *Student Acceptable Use Policy for Electronic Networks* will result in the loss of privileges, disciplinary action, and/or appropriate legal action.**

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

a. Using computers or the network inconsistent with or in violation of District or school rules
b. 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
c. Downloading any programs, files, or games from the Internet or other sources that can be run or launched on the computer as a stand-alone program
d. Using the network for private financial or commercial gain or for the transaction of any personal business or commercial activities; this includes any activity that requires the exchange of money or use of a credit card number, the purchase or sale of any kind, or use for product or service advertisement
e. Wastefully using resources, such as file space
f. Playing games, including Internet-based games, during the instructional day, unless school-approved and teacher-supervised
g. Using online social networks or any form of online publishing or online personal communication during the instructional day unless under the direction of a teacher
h. Streaming non-educational music or video during the instructional day
i. Bypassing or attempting to bypass the District's Internet filtering software. Use of proxy servers to bypass Internet filters or to conceal the identity of one's computer or user information on the network.
j. Creating or using unauthorized networks including, but not limited to voice, data, IP, peer to peer, or proxy networks
k. Hacking or gaining unauthorized access to files, resources or entities
l. 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
m. Using another user's account or password; no student should be using a guest account, but should always use the account provided to them by the District
n. Posting material authored or created by another without his/her consent
o. Posting anonymous messages
p. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material
q. Using the network while access privileges are suspended or revoked.
r. Changing or manipulating system configurations or settings.

Network Etiquette - You are 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 your messages to others.
b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
c. Do not reveal the personal information, including the addresses or telephone numbers, of students or colleagues.
d. Recognize that electronic mail (e-mail) is not private. People who operate the system have access to all mail. 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 the private property of the District.

Vandalism

Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy property. Do not deface or vandalize District owned equipment in any way, or the equipment of another person, including but not limited to, marking, painting, drawing, marring, removing computer parts, or placing stickers on any surface. Do not vandalize data in any way, or the data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

Internet Safety

Each District computer with Internet access shall have 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 federal law and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose, provided the person receives prior permission from the Superintendent or system administrator. No filtering software is one hundred percent effective, and it is possible that the software could fail. In the event that filtering is unsuccessful and users gain access to inappropriate and/or harmful material, the District will not be liable. The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Limiting student access to inappropriate matter as well as restricting access to harmful materials
2. Student safety and security when using electronic communications
3. Limiting unauthorized access, including "hacking" and other unlawful activities
4. Limiting unauthorized disclosure, use, and dissemination of personal identification information

Staff members shall supervise students while students are using District Internet access to ensure that the students abide by the *Student Acceptable Use Policy for Electronic Network Access.*

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

LEGAL REF: No Child Left Behind Act, 20 U.S.C. §6777; 720 ILCS 135/0.01.
Children's Internet Protection Act, 47 U.S.C. §254(h) and (l);
Enhances Education Through Technology, 20 U.S.C §6751 et seq;

Search and Seizure

Students have a limited expectation of privacy with regard to the contents of their personal files and online activity may be monitored while using District's network. Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the District Technology Use Policy. If this occurs and the student disciplinary code, District regulations, employment policy, the collective bargaining agreement and/or the law will be used to resolve the situation. An individual search will be conducted if there is reasonable suspicion that a user has violated the law or the student disciplinary code.

Cell Phone Policy

Phones are not permitted to be used during the school day.
Students are not permitted to use any type of electronic signaling device during class time, passing periods or breaks without the permission of the school administration. The electronic signaling device must remain turned off and in locker during the instructional school day. If a student receives permission by school administration to use an electronic signaling device, it shall not disrupt the educational program. If disruption occurs, the school staff shall direct the student to turn off the device and/or confiscate it.

If a school staff member finds it necessary to confiscate a device, parents will be notified promptly and the device will be returned in accordance with school rules after the administrator or designee has consulted with the student's parent/guardian. The school is not responsible for lost or stolen electronic signaling devices. Students are to make arrangements with their parent(s) or guardian(s) to contact the school office when attempting to reach them during the school day.

The following are inappropriate uses of electronic signaling devices: harassment, threats, intimidation, electronic forgery, cyber bullying/cyber threats, invasion of personal rights, cheating on tests/exams, or other forms of illegal behavior during the instructional and non- instructional day. Students are not to use material or text message to invade personal privacy or harass another person, or disrupt the instructional day, or engage in dishonest acts.

The use of camera phones is strictly forbidden in private areas, such as, locker rooms, washrooms, dressing areas, classrooms, and offices at any time. **Such use may also be in violation of the criminal code.**

Whiteside School District is not responsible for lost or stolen cell phones.

Other Electronic Devices

Possession of personal radios, cassette/CD players, iPods, iPads, mp3 players, Game Boys, and other electronic devices is prohibited on campus, unless school approved and teacher supervised.

Cyber Bullying

Cyber bullying is defined as bullying via the use of the Internet, interactive and digital technologies (such as computer, smartphones, etc.) and/or mobile telephones. The use of any school computer or electronic device for the purpose of cyber bullying is strictly prohibited. Cyber bullying using home-based or off-campus devices that result in a material and/or substantial disruption to the school and/or a true threat will constitute grounds for investigation as to whether or not the use violates applicable law or school rules. Should misuse be determined, the student may receive disciplinary consequences appropriate for the frequency and severity of the violation. We encourage students and parents to notify the Assistant Principal's office of any incidents regarding bullying immediately.

Fees and Charges

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

Using a Photograph or Video of a Student

Pictures of Unnamed Students. Students may occasionally appear in photographs and videos taken by school staff members, other students, or other individuals authorized by the Building Principal. The school may use these pictures, without identifying the student, in various publications, including the school yearbook, school newsletter, and school website. No consent or notice is needed or will be given before the school uses pictures of unnamed students taken while they are at school or a school-related activity.

Pictures of Named Students. Many times, however, the school will want to identify a student in a school picture. School officials want to acknowledge that those students who participate in a school activity deserve special recognition. In order for the school to publish a picture with a student identified by name, one of the student's parents or guardians must sign a consent form. Please complete and sign the *Authorization for Using a Photograph or Video of a Student* form to allow the school to publish and otherwise use photographs and videos, with your child or ward identified, while he or she is enrolled in this school. The consent may be revoked at any time by notifying the Building Principal in writing.

Pictures of Students Taken by Non-School Agencies. While the school limits access to school buildings by outside photographers, it has no crowd control over news media or other entities that may publish a picture of a named or unnamed student. School staff members will not, however, identify a student for an outside photographer.

WHITESIDE SCHOOL DISTRICT #115
2018-2019 SCHOOL YEAR

STUDENT AUTHORIZATION FOR ELECTRONIC NETWORK ACCESS

STUDENT NAME: _____
Last, First *(Please print)*

Student Section

I understand and will abide by the Whiteside School District 115 *Student Acceptable Use Policy for Electronic Networks*. I understand that the district and/or its agents may access and monitor my use of the Internet, including e-mail and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken. In consideration for using the district's electronic network connection and having access to public networks, I hereby release the school district and its board members, employees, and agents from any claims and damages arising from my use, or inability to use the Internet.

USER SIGNATURE: _____ **DATE:** _____

Parent/Guardian Section

I have read the Whiteside School District 115 *Student Acceptable Use Policy for Electronic Networks*. I understand that access is designed for educational purposes and that the district has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the district to restrict access to all controversial and inappropriate materials. I will hold harmless the district, its employees, agents, or board members for any harm caused by materials or software obtained via the network. I accept full responsibility for supervision if and when my child's use is not in a school setting. I have discussed this authorization with my child. I hereby request that my child be allowed access to the Whiteside School District 115 Electronic Network.

PARENT/GUARDIAN NAME *(Please print)*: _____

PARENT/GUARDIAN SIGNATURE: _____ **DATE:** _____

AUTHORIZATION FOR USING A PHOTOGRAPH OR VIDEO OF A STUDENT

Parent/Guardian Section

☐ I grant consent to Whiteside School District 115 to identify a picture of my child or ward, by full name and/or the school he or she attends, in any school-sponsored material, publication, video, or website. This consent is valid for the entire time my child or ward is enrolled in Whiteside School District 115. I may revoke this consent at any time by notifying the Building Principal in writing.

☐ I deny consent to Whiteside School District 115 to include a photo of my child in any school-sponsored material, publication, video, or website, even if my child is not identified by name

PARENT/GUARDIAN SIGNATURE: _____ **DATE:** _____

Pictures of students taken by non-school agencies: While the school limits access to school buildings by outside photographers, it has no control over news media or other entities that may publish a picture of a named or unnamed student. School staff members will not, however, identify a student for an outside photographer.

HANDBOOK RECEIPT

_____ (parent/guardian initials) I have received the Student & Parent Handbook/Agenda and understand that my child and I are responsible for following the rules and policies as stated in the handbook. Note: The handbook may be updated throughout the school year. Notice of handbook amendments will be sent to parents through Skyward and will be published in the monthly Smoke Signals Newsletter.

MOVIE PERMISSION FORM

_____ I give permission for my child to watch "G" and "PG" rated movies as might pertain to the curriculum.

PARENT/GUARDIAN SIGNATURE: _____ **DATE:** _____