STARK COUNTY COMMUNITY DISTRICT #100

Authorization for Technology/Electronic Network Access

Each teacher must sign this Authorization as a condition for using the District's Technology/Electronic Network connection. Each student and his or her parent(s)/guardian(s) must sign the Authorization before being granted access. School Board members, Administrators, and authorized community members are treated like teachers for purposes of this Authorization. Please read this document carefully before signing.

The goal of technology at Stark County School District is to enhance, extend, and enrich the learning process and create new opportunities for teaching and learning. The Administration, staff, and students are encouraged to make use of all technology in order to accomplish these goals and to facilitate diversity and personal academic growth.

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This *Authorization* does not attempt to state all required or prescribed behavior by users. However, some specific examples are provided. **The failure of any user to follow the terms *of the Authorization for Technology/Electronic Network Access* will result in the loss of privileges, disciplinary action, and/or appropriate legal action.** The signature(s) at the end of this document is legally binding and indicates the party who signed has read the terms and conditions carefully and understands their significance.

Terms & Conditions

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

2) Privileges - The use of the District's technology and electronic networks is a privilege, not a right, and inappropriate use will results in a cancellation of those privileges. The Building Administration will make all decisions regarding whether or not a user has violated this *Authorization* and may deny, revoke, or suspend access at any time; his or her decision is final.

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

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

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

c) Unauthorized installation and/or copying of copyrighted software on District computers;

d) Downloading copyrighted material for other than personal use;

e) Using the network for private financial or commercial gain;

f) Wastefully using resources, such as file space;

g) Gaining unauthorized access to resources or entities;

h) Invading the privacy of individuals;

i) Using another user's account or password;

j) Posting material authorized or created by another without his/her consent;

k) Posting anonymous messages;

1) Using the network for commercial or private advertising;

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

n) Using the network while access privileges are suspended or revoked.

4) *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 messages to others.

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

c) Do not reveal the personal 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 private property.

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

6) *Indemnification* — The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation *of this Authorization.*

7) *Security* - Network security is a high priority. If you can identify a security problem on the Internet, you must notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account. Attempts to log-on to the Internet as system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to network.

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

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

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

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

b) Students and staff engaged in producing Web pages must provide Building Administration with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of "public domain" documents must be provided.

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

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

e) Individual student pictures, examples of student work, and pre-arranged group photographs may be published on the web site unless there is an express written request by parents/guardians and the student not to do so.

f) Candid group pictures, crowd shots from school events, etc. may be published on the web site at the discretion of the administration.

11) *Use of Electronic Mail—*

a) The District's electronic mail system, and its constituent software, hardware, and data files are owned and controlled by the School District. The School District may provide access to e-mail for students when appropriately supervised, and in conjunction with the school's curricular goals. The School District will provide supervised access to email for staff members in fulfilling their duties and responsibilities, and as an educational tool.

b) 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 members to an electronic mail account is strictly prohibited. No students are allowed to access private e-mail accounts on school property.

c) 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 message that would be inappropriate in a letter or memorandum.

d) Electronic messages transmitted via the School District's Internet gateway carry with them any 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 this School District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.

e) Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system or Building 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.

f) Use of the School District's electronic mail system constitutes consent to these regulations.

Internet Safety

1. Internet access is limited to only those "acceptable uses" as detailed in these procedures.

2. Staff members shall supervise students while students are using District Internet access.

3. The District network has Internet Access which uses devices that are designed to block entry to depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.

4. The system administrator and Building Principals shall monitor Internet Access.

Teachers and staff members need only sign this *Authorization for Technology/Electronic Network Access* once while employed by the School District. Students and parent(s)/guardian(s) need to sign this *Authorization* upon the student entering Kindergarten, 6* grade, and 9th grade after the initial first signing of all students and parents.

Student Violations; Consequences, Notifications and Appeal:

Students who access restricted items on the Internet shall be subject to the following consequences:

a) First Offense : On the first violation during the school year, a verbal and written "First Infraction" notice will be issued to the student. A copy of the notice will be sent to the parent and a copy provided to the building principal or his/her designee. The student shall forfeit all Internet privileges for a period of three weeks.

b) Second Offense : On the second violation during the school year, a verbal and written "Second Infraction" notice will be issued to the student. A copy of the notice will be sent to the student's parent and a copy provided to the building principal or his/her designee. The student shall forfeit all Internet privileges for the balance of the school year.

Parents may direct school officials to completely deny access of your child's access to the Internet or any use of the technology offered at the school.

Also, each notice shall include a description of the appeal process to be used if a student or parent desires to appeal the issuance of a violation notice.

Appeal Procedures

If a student or parent desires to appeal violation notification, the procedures below apply. All appeals must follow the progression prescribed, unless at the given step both parties consent to advance the appeal to the next step.

1**. First Level of Review** :

If the appeal is for a notification that was initiated by a classroom teacher, facility supervisor or dean, the student or parent must first discuss the situation with that individual in an effort to resolve the appeal. If the notification was initiated by the building principal, Step Two becomes the initial step.

2**. Second Level of Review** :

If Step One does not resolve the situation to the satisfaction of the student and/or parent or if the notification was initiated by the building principal, the appeal shall be made to the building principal. Such appeal shall commence no later than 5 days from the date of the notification.

3. **Third Level of Review** :

If Step Two does not resolve the situation to the satisfaction of the student and/or parent, the petitioning student and/or parent may appeal the action to the District Superintendent or his/her designee. Such appeal shall be in writing and shall be filed no later than 5 days from the date of receipt of the building principal's response.

The Superintendent may withdraw, modify, or leave unchanged the ruling in question. The Superintendent shall respond in writing to the petitioning student and/or parent within 10 days. A copy of the response shall be forwarded to the building principal and a copy shall be placed in the student's temporary record.

4. **Fourth Level of Review** :

If step three does not resolve the situation to the satisfaction of the student and/or parent, the petitioning party may appeal the action to the Board of Education. The Board's hearing procedure as described in the District Policy Manual shall apply. The decision of the Board shall be final.