Student: Acceptable Use Policy

At Minooka 201, we acknowledge that there is an inherent risk with using the internet in a classroom environment. However, we firmly believe that the benefits of using the Internet in a constructive manner, far exceed the risk of inappropriate material being displayed. Minooka 201 takes internet filtering (safe search, etc.) with great importance but acknowledges that no filtering technology is perfect and it will not catch everything.

All use of any Minooka 201 network (and/or any other technology resources) shall be consistent with the District's goal of promoting a safe and efficient learning environment for all. This Acceptable Use Policy (AUP) does not attempt to state all required or prescribed behavior by users, but does show some basic examples. The failure of any staff or student to follow the terms of the Acceptable Use Policy 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.

1. Acceptable Use - Access to the District's network (and/or any other technology resources) must be for the purpose of education or research and be consistent with the educational purposes of the District.

2. Privileges - The use of the district's technology resource is a privilege, not a right, and inappropriate use will result in a revocation of access. The building principal or district office administration will make a decision regarding whether or not a user has violated this Acceptable Use Policy and may deny, revoke, or suspend access at any time.

3. Unacceptable Use - Users are responsible for their actions and activities involving all technology resources. Some examples of unacceptable use include:

a. Using the network (and/or any other technology resource) for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation;
b. Sharing your account or password with others;
c. Downloading copyrighted material for reasons other than personal use;
d. Using the network (and/or any other technology resource) for private financial or commercial gain or fraud;
e. Wastefully using resources, including non-educational streaming or saving personal family photos to district computers;
f. Gaining or seeking to gain unauthorized access to resources or entities;

g. Posting private or personal information about another person and/or invading others' privacy;
h. Gaining unauthorized access to the files of others, or vandalizing the data or files of another user;
i. Using another user's account or password;
j. Posting material authored or created by another without his/her consent
k. Posting anonymous messages;
l. Installing or downloading unauthorized software;
m. Using the network (and/or any other technology resource) for commercial or private advertising;
n. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material;
o. Possessing any data which might be considered a violation of these rules in paper, or digital;
p. Using the network (and/or any other technology resource) while access privileges are suspended or revoked; and
q. Circumventing web content filtering or firewall rules to gain access to websites that are normally blocked, including anonymizers, proxy bypass servers, and secret search engines.
r. Searching for, testing, or sharing ways to circumvent content filtering or classroom management tool management

4. Network Etiquette - Users 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 personal addresses, telephone numbers or other sensitive information of students or colleagues
   d. Understand that a user's actions can be "seen" by administrators of the network. It is likely that someone knows the connections you are making, knows what you are doing and what you viewed while on the network.
   e. 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 will be reported to the authorities.
   f. Do not use the network in any way that would disrupt its use by other users.
   g. Illegal activities are strictly forbidden.

5. Storage - The storing of files must be saved on Minooka 201 district owned computers and servers. The use of flash drives or thumb drives, while acceptable, should only be used as a temporary storage for transportation or backups. Cloud storage, using Google Drive with a

min201.org account is the preferred storage location for all students. Storing classwork on private accounts not associated with Minooka 201 is not permitted.

6. Freedom of Information Act - Student files and records may be searched and produced as part of a Freedom of Information Act (FOIA) response.

7. Printing - Students by default do not have access to printers. If a project needs to be printed, students will be directed by their teacher to share the document with them for printing.

8. 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 users suffer. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or a user's 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, or any costs or charges incurred as a result of seeing or accepting such advice.

9. 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 breach of this Acceptable Use Policy.

10. Security - Network security is a high priority. If a user discovers any sign of network security issues, they must notify the system or building administrator. Do not demonstrate the problem to other users unless asked to do by the system or building administrator. Keep your account and password confidential. Do not use another individual's account or password. Attempts to log on 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.

11. Vandalism - Vandalism will result in cancellation of privileges, other disciplinary action, and restitution for costs associated with hardware, software, and system restoration. Vandalism is defined as any malicious attempt to harm or destroy hardware, software, another user's data, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

12. 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.

13. Google Apps for Education - Google Apps for Education is considered a core requirement for classwork. Minooka 201 uses Google Apps for Education as the primary tool for document creation and collaboration in the classroom thus reducing the need for printed documents.. All files and emails created in the Google Apps for Education environment are searchable by the Superintendent or his designee. This includes the ability to search for common, inappropriate

phrases used in cyberbullying. The use of a personal google or “gmail” or any other account not associated with Minooka 201 is not permitted.

Kindergarten and 1st Grade:
Kindergarten and 1st-grade students will be issued Ipads with protective shells. App installation is managed at the district level and most student work is completed through Seesaw. Students are assigned a Google account, which is used primarily for streamlining authentication to numerous apps.

2nd:
Students in 2nd are given access to document creation and collaboration tools but not email. Effectively, these students will have access to cloud-based word processing and presentation slideshow creation tools and streamlining authentication to numerous apps.

3rd - 8th Grade:
3rd through 8th grade emails for students are configured in a very guarded configuration where students can only email teachers and receive service-type email notifications.

14. Appeal: After a student’s access has been revoked, an appeal by the custodian/guardian to the decision can be made to the Superintendent of Minooka 201 or his designee.

By signing and dating this document:

1. The parent or guardian understands that access to the network (and/or any other technology resource) is designed for educational purposes and that the District has taken precautions to eliminate controversial material. However, he/she also recognizes it is impossible for the District to restrict access to all controversial and inappropriate materials. He/she will hold harmless the District, its employees, agents or Board members for any harm caused by materials or software obtained via the network. He/she will accept full responsibility for supervision if and when the child's use is not in a school setting. He/she has discussed the terms of this Acceptable Use Policy with their child and hereby requests that the child be allowed access to the district's network.

2. The student understands and will abide by this Acceptable Use Policy. He/she further understands that any violation of the regulations above is unethical and may constitute a criminal offense. Should he/she commit any violation, privileges may be revoked, school disciplinary action and/or appropriate legal action may be taken.

If you wish to make any changes to your student's AUP status, you will need to request a new form.

Sign:_____ Date:_____