Ross-Hill Academy
Acceptable Use Policy

Ross-Hill Academy is providing students access to the district's electronic network. This network includes internet access, computer services, computer equipment and related equipment for educational purposes. The purpose of this network is to assist in preparing students for success in life and work in the 21st century by providing them with electronic access to a wide range of information. This document contains the rules and procedures for staff and students' acceptable use of the Ross-Hill Academy electronic network.

Ross-Hill Academy prioritizes protection of all students. School district policies have been developed to enforce guidelines and precautions set forth in FERPA (Family Educational Rights and Privacy Act) and CIPA (Children's Internet Protection Act). Staff, students and families are encouraged to become familiar with these regulations to better enable compliance and protection of students. The user interface for information contained on Ross-Hill's Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by the school district, Wayne RESA, Michigan Department of Education and Federal Department of Education confidentiality guidelines. Examples of confidential information include but are not limited to student/family sensitive data regulated by FERPA, school district or building administration data, management company related. Staff should take all necessary steps to prevent or avoid unauthorized access to this information. For further regulatory information visit:

www.michigan.gov/documents/FERPA_34CFR99_119434_7.pdf.
www.fcc.gov/guides/childrens-internet-protection-act

- The Ross-Hill Academy electronic network has been established for a limited educational purpose. The term "educational purpose" includes classroom activities, career development, and limited high-quality self-discovery activities.
- The Ross-Hill Academy electronic network has not been established as a public access service or a public forum. Ross-Hill Academy has the right to place reasonable restrictions on material that is accessed or posted throughout the network.
- As technology is integrated in the daily educational curriculum, internet access may be a common privilege for students. Parents/guardians opposed to this permission should notify the school immediately. **Student access is a privilege — not a right** — and may be revoked due to inappropriate use of equipment or internet; cyberbullying or other violations of the Anti-Bullying Policy; and/or other conduct prohibited in the Parent & Student Handbook.
- Due to the widespread common usage of internet within educational institutions, it is presumed that staff and students will honor this agreement. The district is not responsible for the actions of students who violate them beyond the clarification of standards outlined in this policy.
- The District reserves the right to monitor all activity on this electronic network. Staff and students will indemnify the district for any damage that is caused by inappropriate use of the network.
- Files stored on the network are treated in the same manner as other school storage areas, such as lockers. Staff and students should not expect that files stored on district servers are private.
- Staff and students are expected to follow the same rules, good manners and common sense guidelines that are used with other daily school activities, as well as the law, in the use of the Ross-Hill Academy electronic network.

General Unacceptable Behavior

While utilizing any portion of the Ross-Hill Academy electronic network, unacceptable behaviors include, but are not limited to, the following:

- Staff and students will not post information that, if acted upon, could cause damage or danger of disruption.
- Staff and students will not engage in personal attacks, including prejudicial or discriminatory attacks.
- Staff and students will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a student is told by a person to stop sending messages, they must stop.
- Staff and students will not knowingly or recklessly post false or defamatory information about a person or organization.
- Staff and students will not use obscene speech or speech in the course of committing a crime such as threats to the president, students, staff members or the school, instructions on breaking into computer networks, child pornography, drug dealing, purchase of alcohol, gang activities, threats to an individual, etc., nor in any manner participate in any appearance which may construe criminal intent.
- Staff and students will not use speech that is inappropriate in an educational setting or violates district rules.
- Staff and students will not abuse network resources such as sending chain letters or "spamming.
- Staff and students will not display, access or send offensive messages or pictures.
- Staff and students will not use the Ross-Hill Academy electronic network for commercial purposes. Students will not offer, provide, or purchase products or services through this network. Staff will adhere to district policy in obtaining appropriate authorization of such.
- Staff and students will not use the Ross-Hill Academy electronic network for political lobbying. Students may use the system to communicate with elected representatives and to express their opinions on political issues, with approval of content/language and authorization by their instructor for academic learning purposes.
- Staff and students will not attempt to access non-instructional district systems, such as the student information systems or business systems. Staff and students will not attempt access to any school district systems or files outside of their specific job-related technical and administrative privileges.
- Staff and students will not use any wired or wireless district network (including third party internet service providers) with equipment brought from home. Example: The use of a home or personal computer on the district network.
- Staff and students will not use district equipment, network, or credentials to threaten employees, students or others, or cause a disruption to the educational program.
- Staff and students will not use the district equipment, network, or credentials to send or post electronic messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another person's or organization's reputation, or illegal.
- Any use that violates public safety or compromises the privacy of legally protected school, administrative, staff, student, resident or citizen information.
- Hacking systems and databases or acting to disrupt systems or cause unnecessary network congestion or application delays.
- Use of any remote control software on any internal or external host personal computers or systems not specifically set up by Ross-Hill Academy technology staff or contractors, using methods authorized or unauthorized by standard or policy of the school district or law.

Bullying, including "Cyberbullying" Is Prohibited

- Bullying of a pupil or group of pupils, at school or a school function/activity is strictly prohibited – **this includes cyberbullying.** All pupils and staff are protected under this policy and subject to the same rights and/or disciplinary actions as other prohibited conduct. Bullying/cyberbullying is

equally prohibited without regard to its subject matter, motivating disposition, intention, animosity or ill will.

- Retaliation or false accusation against a target of bullying, a witness, or another person with reliable information about an act of bullying is strictly prohibited.
- **The school district assures "confidentiality"** of any individual who reports an act of bullying including, but not necessarily limited to students, parents, family members and staff.

The **Bullying/Cyberbullying** policy is an official segment of the school district's Anti-Bullying Policy. Students, parents and staff are encouraged to refer to the Anti-Bullying Policy in its entirety.

E-Mail (Note: Ross-Hill Academy does not grant privileges for student E-mail accounts.)

- E-mail for staff may be provided through the school district. Staff is responsible for adherence to all federal, state and local internet and/or criminal regulations.
- Staff is responsible for professional conduct which respects the legal and moral rights of all students, families, staff members and the Ross-Hill Academy school district.

Telnet and FTP (Note: Telnet and FTP are typically not given to students)

- Telnet and FTP services may or may not be available to students. However, all aspects of this policy are applicable to material accessed or downloaded.

Message Board/Usenet Groups (Note: This access is not typically given to students)

- The district may provide access to selected newsgroups that relate to subjects appropriate for educational use. Messages posted locally that are in violation of this policy will be removed. The district reserves the right to immediately terminate an account for misuse of message boards or Usenet groups.

Real-time, Interactive Communication Areas (Note: Chat rooms are normally blocked)

- Students may use chat or instant messaging, but only under the direct supervision of a teacher to support educational activities with approval by school administration.

Web Sites

- Elementary and Middle School Level - Access to information for students on the web will generally be limited to prescreened sites that are closely supervised by the teacher and/or administration.
- Elementary and Middle School Level - Group pictures without identification of individual students are permitted. Student work may be posted with either student first name only or other school-developed identifier (such as an alias or number).
- High School Level - Access to information for students on the web will generally be provided through prescreened sites and in a manner prescribed by the school.
- High School Level - Students may be identified by their full name with parental approval. Group or individual pictures of students with student identification are permitted with parental approval.
- Material placed on any Ross-Hill Academy general, classroom, or student Web pages are expected to meet academic standards of proper spelling, grammar and accuracy of information and school policy, with approval by the district.
- Material (graphics, text, sound, etc.) that is the ownership of someone other than the school or staff member or student may not be used on web sites unless formal permission has been obtained from the owner(s) and the appropriate school official(s) in accordance with school policy.
- All Ross-Hill Academy student web pages require authorization and should have a link back to the home page of the classroom or school district website.
- Parents reserve the right to object to web publishing of materials identifiable to their child(ren). Staff should take responsible measures towards assuring parental agreement.

Students Personal Safety

- **Students will not share personal contact information about themselves or other people.** Personal contact information includes address, telephone, school address, or work address.
- **Students will not disclose their full name or any other personal contact information for any purpose.**
- **High school students will not disclose personal contact information,** except to education institutes for educational purposes, companies or other entities for career development purposes, or without specific building administrative approval.
- **STUDENTS WILL NOT AGREE TO MEET WITH SOMEONE THEY HAVE MET ONLINE.**
- Students will promptly disclose to the teacher, the supervising staff member, principal or school office any message received that is inappropriate or makes the student feel uncomfortable.

System Security

- Staff and students are responsible for individual accounts and should take all reasonable precautions to prevent others from being able to use them. Student passwords shall be assigned by teachers. Staff temporary passwords shall be assigned by members of the Technology Team and changed to secret personal passwords upon logon. Under no conditions should staff or students provide their password to another person.
- Staff and students must immediately notify a teacher or the system administrator if they have identified a possible security problem. Staff and students should not go looking for security problems, because this may be construed as an illegal attempt to gain access.
- Staff and students will not attempt to gain unauthorized access to any portion of the Ross-Hill Academy electronic network. This includes attempting to log in through another person's account or access another person's folders, work, or files. These actions are illegal, even if only for the purposes of "browsing".
- Staff and students will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.
- Users will not attempt to access Web sites blocked by district policy, including the use of proxy services, software, or Web sites.
- Users will not use sniffing or remote access technology to monitor the network or other user's activity.

Software and Files

- Software is available to be used as an educational resource. No staff or student may install, upload or download software without permission from the district technology department.
- A staff or student's account may be limited or terminated for intentional misuse of software or other applications on any district-owned equipment.
- Files stored on the network are treated in the same manner as other school storage areas, such as lockers. Routine maintenance and monitoring of the Ross-Hill Academy electronic network may lead to discovery that a staff or student has violated this policy or the law. Staff and students should not expect that files stored on district servers are private.

Technology Hardware

- Hardware and peripherals are provided as tools for use for educational purposes. Staff and students are not permitted to relocate hardware (except for some portable devices), install peripherals or modify settings to equipment without the consent of the district technology department. Please check with the district technology department prior to relocating portable devices.

Vandalism

- Any malicious attempt to harm or destroy data, the network, other network components connected to the network backbone, hardware or software will result in cancellation of network privileges. Disciplinary measures in compliance with the district's discipline code and policies will be enforced.

Plagiarism and Copyright Infringement

- **Staff and students will not plagiarize works found on the Internet.** Plagiarism is taking the ideas or writings of others and presenting them as if they were their own.
- Legal policies on copyright will govern the use of material accessed and used through the district system.
- Copyrighted material will not be placed on any system without the author's permission. Permission may be specified in the document, on the system or must be obtained directly from the author.

Videoconference

- Videoconferencing is a way that staff and students can communicate with other students, speakers, museums, etc. from other parts of the country and the world. With videoconferencing equipment, users can see, hear, and speak with other students, speakers, museum personnel, etc., real-time.
- Videoconference sessions may be videotaped by school personnel or by a participating school involved in the exchange in order to share the experience within ours or their building or district, when approved by district administration.
- Staff and students' voices, physical presence, and participation in the videoconference are transmitted to participating sites during each session. Parental notification and/or permission is required. Staff must notify the district administration for authorization. Legal rules and procedures relative to acceptable use and behavior apply during all videoconference sessions.

Student Rights

- Students' right to free speech applies to communication on the Internet. The Ross-Hill Academy electronic network is considered a limited forum, similar to the school newspaper, and therefore the district may restrict a student's speech for valid educational and moral reasons. The district may practice and requires the instructional staff to practice restraints and policy regarding appropriateness of communications through use of school-owned properties and school representation.
- An individual search will be conducted if there is reasonable suspicion that a student has violated this policy or the law. The investigation will be reasonable and related to the suspected violation.

Due Process

- *The district will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the district network.*
- In the event there is an allegation that a staff member or student has violated the district acceptable use regulation and policy, the staff/student will be provided with a written notice of the alleged violation. An opportunity will be provided to present an explanation before a neutral administrator (or staff/student will be provided with notice and an opportunity to be heard in the manner set forth in the disciplinary code).
- Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. Violations of the acceptable use regulation and policy may result in a loss of access as well as other disciplinary or legal action.
- If the violation also involves a violation of other provisions of other school rules, it will be handled in a manner described in the school rules. Additional restrictions may be placed on a student's use of his/her network account.

Limitation of Liability

- The district makes no guarantee that the functions or the services provided by or through the district network will be error-free or without defect. The district will not be responsible for any damage suffered, including but not limited to, loss of data or interruptions of service.
- The district is not responsible for the accuracy or quality of the information obtained through or stored on the network. The district will not be responsible for financial obligations arising through the unauthorized use of the network.

Violations of this Acceptable Use Policy

Violations of this policy may result in loss of access as well as other disciplinary or legal action. Staff shall be subject to applicable employment policy and procedures, and/or legal action and prosecution by the authorities. Students' violation of this policy shall be subject to the consequences as indicated within this policy as well as other appropriate discipline, which includes but is not limited to:

- Use of district network only under direct supervision
- Suspension of network privileges
- Revocation of network privileges
- Suspension of computer privileges
- Suspension from school
- Expulsion from school and/or
- Legal action and prosecution by the authorities

The particular consequences for violations of this policy shall be determined by the school administrators or school board, as applicable. School expulsion, employee termination, and/or legal action or actions may occur as appropriately determined by the school district, Department of Education regulations or other legal authorities.