**ACCEPTABLE USE POLICY FOR Coshocton Opportunity School**

**DISTRICT NETWORK / INTERNET**

The District recognizes that technology can greatly enhance the instructional program, as well as the efficiency of district and school administration. The District also realizes that careful planning is essential to insure the successful and cost-effective implementation of technology-based materials, equipment, systems and networks. Technology devices and use of the district network are provided to enhance instruction and to support student learning. It also is to assist in the administration of the District. All devices are to be used in a responsible, ethical and legal manner. Failure to adhere to this policy and the guidelines listed below will result in the loss of the user's access privileges. Improper use of the District's technologies and systems in violation of this and/or other board policies may result in student or staff disciplinary actions and/or possible referral to the appropriate authorities.

Because our network provides Internet connectivity, users and parents/guardians of users must understand that neither the District, school administration or school staff can control the content of the information available on the Internet. Some of the information available may be considered controversial, offensive, inaccurate, and may be considered harmful. Pursuant to Federal law, the Board has implemented technology protection measures, which protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children’s Internet Protection Act. At the discretion of the Board or the Superintendent/designee, the technology protection measures may be configured to protect against access to other material considered inappropriate for users to access. The Board also utilizes software and/or hardware to monitor online activity of users to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. The technology protection measures may not be disabled at any time that students may be using the Education Technology, if such disabling will cease to protect against access to materials that are prohibited under the Children’s Internet Protection Act. Any student who attempts to disable the technology protection measures will be subject to discipline. However, it is impossible to control access to all material. In addition to filtering at the District and ITC level, all staff members and students district wide will receive Internet safety training through Public School Works modules completed in the Fall of each school year at all grade levels. Students enrolled in technology classes will receive additional Internet safety training through grade level appropriate resources.

The Superintendent or designee may temporarily or permanently unblock access to websites or online educational services containing appropriate material, if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures. Any user may contact the Technology Department through the help ticket system to request that material be unblocked.

Students, parents/guardians, and school employees must be aware that computer use is a privilege and not a right. Privileges will be withdrawn from users who the District determines in its sole discretion do not respect the rights of others or who do not follow the rules and regulations established by the District. A copy of all applicable rules and regulations are provided to all users and are also available in handbooks and on District websites. Students are required to submit an Acceptable Use Policy Agreement form signed by the individual student user as well as the parent and/or guardian of the user which acknowledges the risks and regulations for District network/Internet use.

The Board makes every effort to select and implement products that protect the confidentiality of students’ personally identifiable information and that avoid third party promotional marketing material. In order for students to continue to be able to use the most effective web-based tools and applications for learning, it may be necessary for the Board to provide student data to online educational service providers. In addition to data provided by the Board, online educational service providers may collect additional data using cookies, logs, and other Internet-based technologies. Online educational service providers communicate information about their collection, protection, use and disclosure of data through their privacy policies. The Board utilizes several online educational service providers that are operated by third-parties. For example, students will receive a Google account to participate in the Google Apps for Education program used by the Board. The Board also utilizes other online educational service providers such as, but not limited to EduTyping, Google Apps for Education Suite, Google services, INFOhio resources, IXL, Keyboarding without Tears, Learn21, Meals Plus, Prodigy, ProgressBook, NWEA, Renaissance Learning, ST Math, Think Central, ThinkCERCA. Typing Club, Typing.com and other technology-based resources selected by instructional staff and used for academic purposes.

Under the Children’s Online Privacy Protection Act (COPPA), online educational service providers must provide parental notification and obtain parental consent before collecting personal information from children under the age of 13. COPPA permits school districts to consent to the collection of personal information on behalf of its students for educational purposes. This eliminates the need for the online educational service providers to receive individual parental consent for each student.

Students are personally and solely responsible for the care and security of their electronic communication devices (ECDs). The Board assumes no responsibility for theft, loss, damage, or vandalism to student/parent-owned ECDs brought onto its property, or the unauthorized use of such devices.

The following procedures and guidelines will be adhered to by students, staff, community members, or others who are authorized to use the district's computers and/or on-line services:

The administration reserves the right to monitor all activity on District-owned networks or technologies including the use of district approved resources and other resources at all times. Monitoring may include, but is not limited to, visual observations of online activities during class sessions; or use of specific monitoring tools to review browser history and network, server, and computer logs.

Do not reveal your personal information like your home address, social security number, phone number, account number(s), password(s) or any other personal information or that of other users.

Do not use profanity, obscenity or other language which may be offensive to others. Use appropriate language only.

Use of any District-owned technologies or systems to commit acts of vandalism will result in the immediate cancellation of user privileges. In addition, other disciplinary action, monetary charges for damages, and/or referral to appropriate authorities may result. Vandalism includes but is not limited to: uploading/downloading any inappropriate material, creating or spreading computer viruses and/or any malicious attempt to harm or destroy equipment, materials, or any data, physical destruction of equipment, etc.

Users are expected to report any security problem or misuse of the computers and/or network to the teacher or other appropriate authority such as media center staff, principal, or technology staff member immediately.

Do not violate copyrights or commit plagiarism.

The network should be used correctly and attempts to interfere with others' access to it should not be made.

The user in whose name a network account is issued is responsible for its proper use at all times. They shall use these systems only under their own username and password issued for them by the district. Improper use of the account will result in the loss of access to the account.

Users shall not use any District-owned system or technology for any activity prohibited by law or District policy i.e.: sexual acts or materials, acts or threats of violence, the use of drugs, alcohol or tobacco.

Users shall not access or transmit any material that is obscene, disruptive, sexually oriented, threatening, or that could be considered to be an insult to others based on their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.

All users shall not attempt to read, delete, copy, modify or forge other users' files.

Staff users shall not read other users' mail or files without permission. They shall not attempt to interfere with other users' ability to send or receive electronic mail, nor shall they attempt to read, delete, copy, modify or forge other users' mail or files without permission.

The District network / Internet shall be used only for purposes related to education or operation of the District. Use of the District network or devices for personal financial gain, political activity, commercial activity, or for any illegal activity is strictly prohibited.

To use a device within our network you must sign below that you have read and agree with our guidelines

Student Signature

Parent/Guardian Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date