

## TECHNOLOGY – ACCEPTABLE USE POLICY

### **Statement of Purpose - Acceptable Use Policy for Technology**

The Akron-Westfield Community School District, hereinafter referred to as the “District” uses technology as one way of enhancing its mission to teach the skills, knowledge and behaviors students will need as successful and responsible adults in the community and as life-long learners. Technology includes, but is not limited to, the electronic transfer of voice, video, data and internet connectivity. Technology provides unequalled opportunities to explore and use a varied and exciting set of resources. In order to make these resources available to everyone, those who use the school’s available technology must do so in a way that is consistent with the District’s educational mission.

This *Acceptable Use Policy for Technology* is intended to provide general guidelines and examples of prohibited uses, but does not attempt to state all required or prohibited activities by users.

Students and employees will sign a form acknowledging that they have read and understand the *Acceptable Use Policy for Technology*, that they will comply with the policy, and understand the consequences for violation of the policy.

### **Expectation of Privacy**

The District retains control, and supervision of all technology including computers, networks and Internet services owned or leased by the school. The District reserves the right to monitor all use of technology.

**Each person has no expectation of privacy in their use of the District technology, including email and stored files. All communications and information received via the district technology shall be considered the property of the district. Each person will respect the rights of others to the protection of the files they store on a computer and will not alter or damage such files.**

### **Acceptable Uses**

Access to the District’s technology is provided for educational purposes and research consistent with the school district’s educational mission, curriculum and instructional goals. The same rules and expectations which govern conduct and communication shall also govern individual use of technology. Individuals are further expected to comply with these rules and all specific instructions utilizing the school district’s technology. Technology use is a privilege, not a right.

### **Unacceptable Uses**

Examples of unacceptable uses that are expressly prohibited include, but are not limited to, the following:

1. **Inappropriate Use of Technology (24/7)** - Accessing, submitting, posting, publishing, forwarding, down loading, scanning or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal;

2. **Inappropriate Use of Technology During the School Day** - Accessing sites for personal financial gain (i.e. online gambling), commercial transactions (i.e. online shopping, eBay, etc.), or gaming software or sites except with direct teacher authorization;
3. **Unauthorized access to Social Networking/Chat Rooms/News Groups During the School Day** - Accessing social networking sites or software, chat rooms or news groups without specific authorization;
4. **Inappropriate Use of Cameras or Other Recording Devices** - Computers and other technology are not to be used to take pictures or video without the consent of all persons being photographed or recorded;
5. **Illegal Activities** - Using the District's technology, including computers, networks, Internet services and other technology equipment for any illegal activity or that violates other Board policies, procedures and/or school rules;
6. **Violating Copyrights** - Copying or downloading copyrighted material without the owner's permission (i.e. using copyrighted music in a project);
7. **Plagiarism** - Representing as one's own work any material obtained from other sources (such as term papers, articles, etc). When Internet sources are used, the author, publisher and Web site must be identified;
8. **Copying Software/Media Files** - Copying or downloading unauthorized software; illegally downloading music, photos, movies, games or other such files;
9. **Misuse of Passwords/Unauthorized Access** - Sharing passwords, using other users' passwords without permission and/or accessing other user accounts;
10. **Malicious Use/Vandalism** - Any malicious use, disruption or harm to the District's computers, networks, Internet services, and technology resources, including but not limited to hacking activities and creation/uploading of computer viruses;

### **Consequences**

The use of the District's technology, including laptops, Internet access, is a privilege, not a right. Compliance with the District's *Acceptable Use Policy for Technology* is mandatory. Users who violate this policy may have their computer/technology privileges limited, suspended, or revoked. Such violations may also result in disciplinary action, referral to law enforcement and/or legal action. The building principal or his/her designee shall have the final authority to decide whether a user's privileges will be limited, suspended or revoked based upon the circumstances of the particular case, the user's prior disciplinary record and any other pertinent factors.

### **Responsibility**

The District utilizes electronic systems which are Children's Internet Protection Act (CIPA) compliant and other methods to regulate student and employee technology use. These monitoring methods do not guarantee compliance with this policy. **The user understands that their activities may be monitored when logging onto district owned technology.** The District assumes no responsibility for the accuracy of information found on the internet or for any unauthorized charges made by users, including but not limited to credit card charges, long distance telephone charges, equipment and line costs, or for any illegal use of its computers such as copyright violations.

It is the sole responsibility of the user to backup data as necessary.

The security of the school's technology resources including computers, networks and Internet services is a high priority. Any user who identifies a security problem must notify his/her teacher or network administrator immediately. The user shall not demonstrate the problem to others or access unauthorized material. Any user who attempts to breach system security, causes a breach of system security or fails to report a system security problem shall be subject to disciplinary and/or legal action in addition to having his/her computer privileges limited, suspended or revoked.

All users of District technology agree to indemnify the school or district against any losses or damages that occur out of violations of this *Acceptable Use Policy for Technology*.

Legal references: Iowa Code 279.8 (2009)

Approved \_\_\_\_\_

Reviewed \_\_\_\_\_

Revised \_\_\_\_\_