Digital Technology Acceptable Use Policy and Conduct Agreement

(revised March 15, 2016)

Introduction

East Alton – Wood River Community High School District #14 recognizes that access to technology in school gives both students and teachers greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st century technology and communication skills.

To that end, we provide access to technologies for student and staff use. This Acceptable Use Policy outlines the guideline and behaviors that users are expected to follow when using school technologies or when using personally owned devices on the school campus.

- EAWR District 14's network is intended for educational purposes.
- All activity over the network or using district technologies may be monitored and retained.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources can result in disciplinary action.
- EAWR District 14 makes a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from misuse of school technologies.
- Users of the EAWR District 14 network or other technologies are expected to alert technology staff or administrators immediately of any concerns for safety or security.

Technologies Covered

EAWR District 14 may provide age-appropriate technologies to students and employees for the purpose of supporting curriculum, instruction and assessment.

Usage Policies

All technologies provided by EAWR District 14 are intended for educational purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Web Access

EAWR District 14 provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow protocol to alert an administrator, staff member, the Educational Technology Director, or submit the site for review.

Email

EAWR District 14 may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.

If users are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the district policy or the teacher. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Social/Web 2.0/Collaborative Content

Recognizing that collaboration is essential to your education, EAWR District 14 may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally identifying information online.

Mobile Devices Policy

EAWR District 14 may provide users with mobile computers or other devices to promote learning both inside and outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to the Educational Technology Director immediately. Users may be financially accountable for any damage resulting from negligence or misuse.

Use of school-issued mobile devices, including use of the school network, may be monitored.

Personally-Owned Electronic Devices

Students are prohibited from using any personal electronic devices (e.g. cell phones, smartphones, iPads and other tablet computers, laptops, etc.) or similar devices during class periods (whether indoors or outdoors) unless being used for educational purposes determined and expressly authorized by a teacher or the administration for a specific educational purpose during a specified period of time, place, and manner. This ban also includes "behind-the-wheel" driving. During those class periods, in which the teacher or administrator has not expressly authorized the use of personally-owned electronic devices, students may carry them in backpacks, purses, or jackets.

Students may use personal electronic devices during passing periods and lunch periods, provided their use does not infringe on the rights of other students or staff; endanger the safety or welfare of the owner or other students and/or staff; and abide by all of the rules regarding the use of electronic devices, as stated elsewhere in this agreement.

The district is not responsible for loss, theft, damage, or vandalism to any of these devices.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs of unknown or untrusted origin. If you believe a computer or mobile device you are using might be infected with a virus, please alert the administration. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Downloads

Users should not download or attempt to download or run any executable or installer programs such as .exe or APPS over the school network or onto school resources without express permission from the Educational Technology Director. You may be able to download other file types, such as images of videos. For the security of our network, download such files only from reputable sites, and only for educational purposes.

Netiquette

- Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.
- Users should also recognize that among the valuable online content, there is also unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.
- Users should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it's out there—and can sometimes be shared and spread in ways you never intended.

Plagiarism

- Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet.
- Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff; parent or guardian) immediately.

- Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult supervision.
- Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others.
- Users should never agree to meet someone they meet online in real life without parental permission.

Cyber-bullying

Cyber-bullying will not be tolerated. Harassing, flaming, demeaning, impersonating, outing, tricking, excluding, and cyber-stalking are all examples of cyber-bullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyber-bullying can be a crime. Remember that your activities are monitored and retained.

Examples of Acceptable Use

I will:

- Use school technologies for school-related activities and research.
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat school resources carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts) online.

- Use school technologies at appropriate times, in approved places, for educational pursuits only.
- Cite sources when using online sites and resources for research; ensure there is no copyright infringement.
- Recognize that use of school technologies is a privilege and treat it as such.
- Be cautious to protect the safety of others and myself.
- Help to protect the security of school resources.

This is NOT intended to be an exhaustive list. Users should use their own good judgment when using any technologies.

Examples of Unacceptable Use

I will **not**:

- Use technologies in a way that could be personally or physically harmful to others or myself.
- Search for inappropriate images or content.
- Engage in cyber-bullying, harassment, or disrespectful conduct toward others—staff or students.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use technologies to send spam or chain mail.
- Plagiarize content I find online.
- Post personally identifying information, about myself or others.
- Agree to meet someone I meet online in real life.
- Use language online that would be unacceptable in the classrooms (including inappropriate acronyms, initials, or emoticons)
- Use technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, accounts, or content that isn't intended for my use.

This is NOT intended to be an exhaustive list. Users should use their own good judgment when using any technologies.

Limitation of Liability

- EAWR DISTRICT 14 will not be responsible for damage or harm to persons, files, data, or hardware.
- While EAWR DISTRICT 14 employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.
- EAWR DISTRICT 14 will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges in extreme cases
- Notification to parents in most cases
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution

I have read and understood this Acceptable Use Policy and agree to abide by it:

_____
(Student Printed Name)

_____
(Student Signature)

_____
(Date)

I have read and discussed this Acceptable Use Policy with my child:

_____
(Parent/Guardian Printed Name)

_____
(Student/Guardian Signature)

_____
(Date)