Westfield Public School District
Student Acceptable Use of Technology Agreement

The Westfield Public School District believes technology, including computers, electronic devices and the Internet, provides access to vast, diverse and unique resources in a global community. Our goal in providing electronic tools, a computer network and Internet access to teachers, staff and students is to promote educational excellence by facilitating resource sharing, communication and enabling new types of educational pursuits. All users are encouraged to use technology to pursue intellectual activities, seek resources, access libraries, collaborate and engage in learning activities however, it is important to remember that access is a privilege, not a right, and the user is responsible at all times for its proper use.

ACCESS TO ONLINE MATERIALS

Educational Purpose: The materials accessed by students through the district's Internet system should be for class assignments or for personal research on subjects similar to that studied in a class or in the school library. A student may not attempt to access any Internet resource without the prior consent of the teacher. The Internet is an extension of the classroom and teachers are responsible for and must be aware of where his/her student goes on the Internet. Use for entertainment purposes is not allowed.

Content Filtering: In order to be in compliance with the Children's Internet Protection Act (CIPA), filtering software has been installed throughout the City of Westfield's Wide Area Network. This software blocks access to visual depictions of material that is obscene or otherwise considered harmful to minors. Realizing that no filtering software is perfect, we cannot however guarantee that users will not encounter text, pictures or references that are objectionable. Students who try to access appropriate sites which are blocked, should report this to a school librarian, computer lab coordinator, principal, or teacher. Proxy sites or other technologies cannot be used to bypass the filtering software.

Students are responsible for avoiding access to inappropriate material and reporting incidents should they occur.

Prohibited Internet uses include, but are not limited to:

a) Any violation of federal, state and local law.

b) Accessing threatening, offensive or profane material. Offensive content includes, but is not limited to sexual comments or images, racial slurs or other comments that may offend someone on the basis of his/her age, gender, race, sexual orientation, ethnic background, religious beliefs, national origin or disability.

c) Using a computer to provide services to others for profit.

d) Committing plagiarism by taking the ideas or writings of others and presenting them as if they are your own.

e) Committing copyright infringement by inappropriately reproducing a piece of work that is protected by a copyright.

f) Committing vandalism by attempting to harm or destroy network resources, data of another user, the Internet, or other networks, including the creation of, or uploading of, computer viruses on the Internet or host site.

g) Using another individual's network access including use of another individual's network username and password without authorization.

h) Consuming large amounts of bandwidth, resulting in disruption of the network, including but not limited to:
   - Network/Internet games
   - Streaming video and audio for non-educational purposes
   - Non-educational teleconferencing
   - Downloading very large files without prior approval of technology staff

ELECTRONIC COMMUNICATION

As part of 21st century learning, teachers and students will be using Web tools including, but not limited to email, blogs, wikis, podcasts, videocasts and virtual classrooms. These technologies improve student communication and collaboration skills, provide a real audience and extend learning beyond the classroom walls while building digital citizenship skills. The following terms and conditions relate to these New Web Tools.

Privacy and Communication Safety Requirements:

- Most electronic communication is a matter of public record and should never be considered private or secure
- Students will act safely by keeping personal information about themselves or others out of Web projects. This information includes last names, personal email addresses, home addresses, phone numbers, school names or other information that could help locate someone in person. No identifying photos or videos can be posted without proper permission.
- Students will treat blog and wiki spaces as they would a classroom space, and use appropriate and respectful language. Posts, including pictures and videos, must be school-appropriate.
- When posting a link in a blog, podcast, videocast or wiki, students must first read the information carefully to be certain that it is appropriate for the school community.
- Students will promptly disclose to a teacher or other school staff member, any form of electronic communication that is inappropriate or makes them feel uncomfortable. Students should not delete such messages until instructed to do so by a staff member.

Publishing of Photos,Video and Student Work:

- Parental permission **must** be obtained for the publishing of student work at each grade level.
- Published documents cannot include any personal information about staff or students.
- **Unidentifiable** photos of K-12 students and teachers may be published on school websites, illustrating school projects and achievements.
- **Unidentified** photos and video (face clearly visible, no name) of K-12 students may be published on school websites, illustrating school projects and achievements, with parent permission.
- **Unidentified** photos and video (face clearly visible, no name) of district teachers and staff may be published on school websites, illustrating school projects and achievements, only with their permission.

Unauthorized use of electronic communication includes, but is not limited to:

a) Accessing social media or blogging sites, without prior approval of a teacher.

b) Creating and exchanging offensive, harassing, obscene, or threatening messages.

c) Creating and exchanging communications that use impolite, abusive, or objectionable language.

d) Impersonating any other person, entity, or organization.

e) Posting information that could cause damage or a danger of disruption to the student's school or any other organization or person.

SECURITY AND SAFETY

Privacy

All student use of the Internet will be supervised and monitored. The district's monitoring of Internet usage can reveal all activities students engage in using the district Internet system. Network and Internet access is provided as a tool for education. The District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the District and no user shall have any expectation of privacy regarding such materials.

Password Protection:

Students are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use their account. Students must not compromise the privacy of their password by giving it to another student or exposing it to public view.

Personally-owned devices:
Users should not connect or install any personally owned computer hardware or hardware components to or in the district's technology resources without the prior approval of the appropriate school/district technology personnel.

Personally-owned devices that are connected to the network must be used in compliance with this Acceptable Use Policy.

The District is not responsible or liable for issues and/or damages caused by the connection of personal devices to the District's network.

Limitation of Liability:

The district will not guarantee that the functions or services provided through the district Internet service will be without error. The district will not be responsible for any damages suffered, including but not limited to loss of data, interruptions of service, or exposure to inappropriate material or people. The district will not be responsible for the accuracy or quality of the information obtained through the system. The district will not be responsible for financial obligations arising through the unauthorized use of the system. Parents can be held financially responsible for any harm that may result from their child's intentional misuse of the system.

BEHAVIORS AND CONSEQUENCES

Appropriate Codes of Conduct and Disciplinary Measures are outlined in school handbooks and the Westfield School District Policy Manual. Any violation of the agreement may result in a cancellation of network privileges and/or disciplinary action. The network administrators may deny access at any time as required. The administration, faculty and staff of the Westfield Public Schools may request the network administrators to deny, revoke, or suspend specific student privileges. Any student identified as a security risk or having a history of problems with other computer systems may be denied access to the Westfield Wide Area Network/Internet.

The District has no duty to regulate or review off-campus Internet messages, statements, postings, or acts but adds that when those acts threaten violence against another student or otherwise disrupts the learning environment or orderly conduct of the school, the school can take action.

STUDENT AND PARENTAL CONSENT

Student use of telecommunications and electronic information resources will be permitted upon submission of consent forms, signed by students and by parents/guardians of minor students.

First Reading: July 7, 2010
Second Reading: July 7, 2010
Adopted: July 7, 2010