

## ACCEPTABLE USE AND INTERNET SAFETY POLICY FOR STUDENTS, STAFF AND GUESTS

### I. **Statement of Purpose**

The Evansville Community School District (District) provides an Information Technology (IT) Network/System to students, staff, and guests to enhance teaching and learning and to facilitate communication. To that end, the District will set high expectations for network users by:

- Increasing student achievement through instructional integration of technology;
- Developing students who are career-ready and life-long learners;
- Continually improving professional development and curriculum materials that are accessible, realistic, and usable by all;
- Providing and supporting a well-planned infrastructure that is able to respond to the rigorous demands of integrated technology;
- Promoting the ethical use of technology; and
- Providing an environment of support and respect.

By accessing the District IT Network (computers, servers, networking equipment, software programs and electronic communication), users can build the skills necessary for success as life-long learners in a rapidly-changing world.

It is the purpose of this policy to advise users about District guidelines for acceptable use of District IT Network/Systems, personal property and accompanying privileges and disciplinary consequences for misuse. Before the District provides network access, students and staff must agree to abide by this policy by submitting their signed consent.

### II. **Acceptable Use**

The District IT Network is an important learning resource which must be accessed responsibly in order to maintain a positive learning environment. Individual users must be sensitive to the impact their actions may have across the network.

- The District IT Network resources will be used to support teaching and learning consistent with District education goals.
- The District will comply with Wisconsin statutory requirements and administration rules related to technology.
- Network users will have no expectation of privacy on the District IT Network or on any device that is connected to it, including personal property.

### III. **No Guarantee/Liability**

The District does not guarantee the permanence or reliability of the IT Network or the accuracy and quality of information obtained through its services.

The District will not assume responsibility for the loss of information or damage to any devices connected to District IT Network by any user. Nor will it accept responsibility to pay users for any claims, losses, or expenses incurred as a result of accessing the District IT Network.

#### IV. **Security**

District IT Network security ensures system stability and protects system users and district data.

Staff must notify the technology department if they find a possible security problem on the IT Network. Students and guests must notify a teacher or principal. Do not demonstrate the problem to other users.

Hacking and other illegal activities are prohibited. Using the District's IT Network and Internet access to gain unauthorized access to other computers or computer systems is prohibited.

Users are responsible for their individual account activity and must not share their passwords and account information with others.

#### V. **Netiquette**

When communicating electronically, user etiquette must be appropriate and polite, as if one were speaking face-to-face with somebody.

The use of on-line social network sites and other Web 2.0 tools will be allowed for valid school related purposes in a directly supervised setting. All other uses are prohibited.

Staff shall not post any information regarding students on Internet sites that are not created for school related purposes. Student information may be posted as referenced in District policy. In addition, staff shall not link to or accept students as "friends" on personal social networking sites, Web 2.0 forums and gaming networks that are not for educational purposes. Any Internet communication (e.g. sites, pages, blogs or Wikis) created for a school related organization or department need to be preapproved by the building administrator. Any Internet communication that was not approved will be asked to close, shutdown or remove the Internet communication.

Cyberbullying is harassment and/or intimidation through the use of digital media/devices. System users will not use electronic technology to bully or harass another individual. Harassment includes repeatedly acting in a manner that annoys or upsets another person or knowingly posting hurtful information about a person or organization.

The District will provide instruction on standards of Internet safety regarding the appropriate use of social networking sites and communication tools, including the dangers of cyberbullying and sharing inappropriate and/or obscene media. To guard personal safety, users should not reveal personal information such as last name, address or telephone number. The system will not be used to access or transmit information that can be considered to be offensive, obscene, or harmful to minors.

#### VI. **Copyright**

System users will abide by the District copyright policy. Further, pirating, which is the illegal copying, downloading, installing or selling of software or copyrighted material, is prohibited. District IT Network users must adhere to software licensing requirements for the District-purchased programs and personally-purchased programs that have been approved to run on District equipment. Copyright laws that regulate the public showing of films also

apply to “video-on-demand” (e.g. Netflix) and personal copies of copyrighted movies and music. Consult the school library media specialist for licensing information.

**VII. Monitoring**

Routine maintenance and monitoring of the District IT Network may reveal that a user was or is violating the District’s acceptable use policy or the law. If such an infringement were to occur, an individual investigation would be requested by the district administrator or his or her designee. Network users are reminded that any materials stored on the District’s IT Network may be discoverable and subject to release under state public open records laws.

**VIII. Personal Property**

Personally owned electronic devices may access the Internet through the District IT Wireless Network. Users will adhere to all policies that apply to the use of the system. Personal property may be searched and/or confiscated if the District has a reasonable suspicion that policy has been violated or there is a safety threat. Personal devices connecting to the District’s IT Wireless Network must be used for educational purposes and may not interfere with instruction or disrupt the learning environment.

**IX. Privileges/Discipline**

The District will cooperate fully with local, state, and federal officials in any investigation concerning or relating to any illegal activities conducted through the system.

In the event there is an allegation that a user has violated the District acceptable use policy or other rules and policies, an investigation will take place and the user will be given due process rights.

- Staff discipline shall be governed by relevant District policies and/or master agreements;
- Students will be given the opportunity to be heard as outlined in the student handbook for each school. Student disciplinary consequences will be individualized to meet specific concerns related to the violation and help the student develop the self-discipline necessary for appropriate use of technology.

Guest user accounts may be suspended with or without notice.

- Legal Ref.: Sections 118.001 Wisconsin Statutes (Duties and Powers of School Boards)  
118.125 (Pupil Records)  
120.12(1) (School Board Duties)  
120.13(1) (School Board Powers)  
943.70 (Computer Crimes)  
943.70(2) (Computer Crimes)  
944.21 (Obscene Material or Performance)  
947.0125 (Unlawful Use of Computerized Communication Systems)  
947.013 (Harassment)  
Children’s Internet Protection Act  
Neighborhood Children’s Internet Protection Act  
Children’s Online Privacy Act  
Family Educational Rights and Privacy Act  
Federal Copyright Law (17 U.S.C.)  
Technology Education and Copyright Harmonization Act (TEACH Act)

Electronic Communications Privacy Act (I 8 U.S.C § 2510-2522)  
Federal Family Educational Rights and Privacy Act  
Broadband Data Improvement Act of 2008 (Title II)  
Chapter 19, Subchapters II and IV General Duties of Public Officials  
Chapter Adm, 12 Wisconsin Administrative Code  
Electronic Records Management – Standards and Requirement

Local Ref.: Policy #771-Copyright Compliance  
Policy #347-Exhibit Student Records Notice  
Policy #536.2-Suspension and Dismissal  
High School Student Handbook  
J.C. McKenna Middle School Student Handbook  
Theodore Robinson Intermediate School Student Handbook  
Levi Leonard Elementary School Student Handbook