



## **INTERNET SAFETY – Policy 6:235**

The Board of Education of Township High School District 214 (“Board”) has adopted the following policy in accordance with the Children’s Internet Protection Act and the Neighborhood Children’s Internet Protection Act (P.L. 106-554).

This policy provides for the monitoring of the online activities of minors, and addresses the following areas:

- use of technology measures to restrict minors’ access to materials harmful to minors and/or inappropriate;
- the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- unauthorized access, including so-called “hacking,” and other unlawful activities by minors online; and
- unauthorized disclosure, use and dissemination of personal information regarding minors.

### Section I. - Curriculum

By being connected to the Internet, students and staff have potential access to electronic mail communication; to information via the World-Wide Web; and to various research sources including certain university library catalogs, the Library of Congress, and other research databases. Access to the Internet and Township High School District 214’s (the “District’s”) network is a privilege and is not a public forum for general use. Employees and students may load District- assigned student work onto the District’s network. However, employees and students shall not load onto the District’s network or Internet any unlawful, inappropriate, or copyrighted works that are not in accordance with fair use guidelines. Employees will not use personal social networking sites to communicate/interact with students. The Board disclaims any responsibility for any information, including its accuracy or quality, obtained or transmitted through use of the Internet. Further, the Board disclaims responsibility for any information that may be lost, damaged or altered or unavailable when using the District’s network. Employees and students shall be solely responsible for any unauthorized charges or fees resulting from their access to the Internet.

### Section II. - Use of Technology Protection Measures

It is the policy of the Board of Education, through the use of internet filtering or blocking devices, to comply with the Children’s Internet Protection Act. Such filtering or blocking device shall be used on all District computers with internet access and during all use of such computers, except as specifically provided below.

It shall be the responsibility of the administration of the District to assess those filtering or blocking devices available for use and to determine the filtering device most effective and appropriate for the School District’s needs.

The Superintendent or Superintendent’s designee may, on a case by case basis, authorize the disabling of filtering or blocking devices to permit adults to engage in bona fide research or for other lawful purposes. Disabling requests will not be granted if the Superintendent determines that the potential harm or disruption incident to the request outweighs its educational or professional

benefit.

All online activities of students and minors may be monitored by those school officials with direct supervisory responsibility for those activities. In addition, school officials may monitor students' and minors' online activities on District computers when not under the direct supervision of school staff. Such monitoring may consist of (i) direct observation of online activities; (ii) review of internet logs and other use records; (iii) generation of internet activity reports or summaries; or (iv) any other method that the Superintendent determines provides for the effective review and monitoring of online activities.

### Section III. - Access to Inappropriate Materials on the Internet and the World Wide Web

It is the policy of the Board, to the extent permitted by law, to limit access by minors to inappropriate matter on the Internet and the World-Wide Web. This policy shall be accomplished through (i) the use of the filtering or blocking devices described in Section II, (ii) enforcement of the District's responsible use of technology policy, and (iii) providing education and counseling to minors and students who use the District's computer system regarding the proper use of internet resources.

### Section IV. - Electronic Mail, Chat Rooms, Social Networking Websites, and Other Forms of Electronic Communications

It is the policy of the Board to ensure the safety and security of minors when using electronic mail, chat rooms, social networking websites, and other forms of direct electronic communications. For this purpose, school officials may regularly review minors' online and internal communications on the District's computer network to assure the safety of students and minors. School officials may further communicate to minors, through the District's student handbook, its acceptable use policy, or other means, information regarding the safety risks raised by online communications and appropriate practices to protect against these risks.

Student use of social media and technologies for school purposes or in a manner that is considered to have a nexus to the District or the school are subject to disciplinary action in accordance with existing board policies, the student discipline code and the responsible use policy.

### Section V. - Cyberbullying, Hacking, Unauthorized Access, and Unlawful Activities of Minors Online

Minors who use the District's computer network shall be permitted to do so only for authorized purposes and for lawful activities. This policy applies to (i) access to the District's own computer network, and (ii) access by minors to other networks and computers when using the District's network. School officials may communicate these restrictions to minors through the District's student handbook, responsible use policy, or other means. Unlawful or unauthorized online activities are identified as forms of misconduct subject to discipline under the School District's student discipline code.

### Section VI. - Unauthorized Disclosure, Use and Dissemination of Personal Information

It is the policy of the District, consistent with State and Federal student records laws, to protect students and minors against the unauthorized disclosure, use and dissemination of personal information through the District's computer system. Users of the District's computer system shall be prohibited from disclosing personally identifiable information regarding students or minors outside the District's computer system, except in specifically authorized instances. This prohibition shall apply to all electronic communications either directed to non-District computers or accessible to non-District users, such as web page postings and other internet-accessible files.

### Section VII. - Definitions

Terms used in this policy shall have the meanings set forth in the Children's Internet Protection Act. The use of the term "Internet" or "network" in this policy refers to all information accessed through the District's network from the various sources as identified above and any and all information accessed

using the District's means of access.

ADOPTED: August 2021

