Policy 6:235 – Exhibit – Authorization for Use of Computers and Electronic Networks

District 203 is committed to educational excellence. Students need to collect and synthesize information from a variety of digital sources, as well as collaborate and communicate with peers and colleagues in a global community. The District will assist students in developing the skills and knowledge to navigate this rapidly-changing world. Additionally, the District will reinforce the ideals of digital citizenship and what it means to access various devices, tools, networks, technologies and apply the Internet responsibly. This document pertains to any and all district-issued "computers," "electronic devices," "mobile devices," and each of these is interchangeable for the purposes of this policy exhibit.

The contents of this exhibit and authorization forms are aligned with the District Policy *6:235*, *Access to District Computers and Electronic Networks* to promote the appropriate and responsible use of technology in support of the District's mission and goals. Additionally, other relevant District policies play a role in the successful use of District computers and electronic networks, including but not limited to: *6:235 AP-1* on *Acceptable Use of District Computers and Electronic Networks* and *7:180* on *Preventing Bullying, Intimidation, and Harassment*. Any employee, student, or other individual engaged in activity that involves the use of the District's electronic resources (systems and/or network and/or district-issued computer (or personal computer for school use)) must comply with the established Board of Education policies as well as these supplemental guidelines and all relevant state and federal laws. Said laws and policies are subject to change without notice.

Terms and Conditions

Access to the District's systems and network must be in support of education and/or research, and be consistent with the educational goals of the District. The terms and conditions of Acceptable Use do not attempt to state all required behavior by students; however, some specific examples are provided. The failure of a student to follow these guidelines may result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Unacceptable Use
- Attempting to harm or destroy District systems or network equipment, data.
- Attempting to harm or destroy the data or device of another student or user of District systems and network.
- Attempting to degrade or disrupt District systems or networks by downloading or modifying malware is vandalism and may constitute a criminal act under applicable State or Federal laws.
- Using District systems or network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State law.
- Unauthorized downloading of software.
- Downloading or storing plagiarized, copyrighted, or materials protected by trade secrets.
- Using District systems and network for private financial or commercial gain.
- Wasting District electronic resources, such as file space, printing or excessive bandwidth.
- Gaining unauthorized access to files, resources, or entities.
- Invading the privacy of individuals, including unauthorized disclosure, dissemination, and use of information, or posting anonymous messages.