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.

- Participating in blog posts, web posts or discussion forums that violate State or Federal law.
- Fraudulently using another student's account or password.
- Posting material authorized or created by another without consent.
- Using District systems or network for commercial or private advertising.
- Intentionally downloading malware, for any reason, including viruses, trojans, worms, password crackers, or any other product intended to bypass District security or Acceptable Use Guidelines.
- Accessing, submitting, posting, publishing, texting or displaying any defamatory, inaccurate, abusive, profane, obscene, sexually oriented, threatening, racially offensive, harassing, bullying or illegal activities.
- Using District systems or network while access privileges are suspended or revoked.
- Using District systems or network as a gateway or intermediate transit point to load data onto a remote, non-District or personal device.
- Modifying or changing system configurations without appropriate permissions.

Any student repeatedly posing a security risk to District systems or networks may be subject to disciplinary action in accordance with existing District discipline policies. Additionally, the District may take disciplinary action for conduct initiated and/or created off-campus involving the inappropriate use of the Internet or web-based resources, if such conduct poses a threat or substantially interferes or disrupts the operations and good order of the District's schools and venues, including student harassment and/or bullying, regardless of whether the action involved the use of District systems and network.

General Usage

No warranties of any kind, whether expressed or implied, are made for the service provided by District systems or network. The District will not be responsible for any damages resulting from loss of data due to service interruptions caused by its negligence or the student's errors or omissions.

Security of all District systems and network is paramount and multiple processes and programs are constantly run to monitor and report security risks. Participation in these security processes and programs is mandatory, and all devices connected to the District network, whether District-issued or personal (for school-use), must submit to associated security scans and sweeps. Students can support this critical security posture by keeping all login names and passwords confidential. If a student suspects or discovers a security risk, that risk must be immediately reported to their teacher who will notify the school Computer Support Associate.

Digital Citizenship

Digital Citizenship is the concept of educating all students in the appropriate use of technology. A good digital citizen is one who knows what is right and wrong, exhibits intelligent technology behavior, and makes good choices when using technology.

All students are expected to abide by the generally accepted rules of network etiquette and conditions of Good Digital Citizenship. These include, but are not limited to:

1. **Respect Yourself.** Select online names that are appropriate, and consider the information and images posted online. Make considered decisions about posting any personal information regarding life experiences, experimentation, and relationships. Recognize that electronic mail (e-mail), in all forms, is not private and that the District reserves the right to access District provided e-mail as well as all other District data systems without notice or permission. If discovered, messages or data relating to, or in support of, illegal activities may be reported to the legal authorities.
2. **Protect Yourself.** Ensure that the information, images, and materials posted online will not put you at risk. Do not publish personally identifiable information such as addresses, phone numbers, birthdates, Social Security numbers, contact details, personal schedule of activities, etc. Report any attacks or inappropriate behavior. Protect accounts, passwords, and resources, and change passwords in compliance with District policy. Never provide District login or password information over e-mail to anyone for any reason. Be aware that the District will never send an e-mail asking for information regarding any kind of security information such as a login name, password, etc.
3. **Respect Others.** Do not use electronic means to antagonize, bully, harass, or stalk others. Do not visit sites that are degrading, pornographic, racist, or otherwise inappropriate. Do not abuse rights of access, and do not enter other people's private spaces or areas. Be polite and do not become abusive in messages to others. Do not swear, or use vulgarities or any other inappropriate language. Do not use District systems or network in any way that would disrupt its use by others.
4. **Protect Others.** Report abuse and do not forward inappropriate materials or communications. Be aware of, and avoid, unacceptable materials and conversations. Do not reveal personally identifiable information of students or colleagues.
5. **Respect Intellectual Property.** Request permission to use resources. Cite any and all use of websites, books, and media. Acknowledge primary sources and validate information. Use and abide by fair use rules.
6. **Protect Intellectual Property.** Request permission to use software and media that others produce. Do not steal software and use only software that the District has purchased, licensed, and registered. Act with integrity and acknowledge that all communications and information accessible via District systems and network are private property.

No Expectations of Data Privacy

The District reserves the right to access and disclose the contents of any account on any District system, including those hosted externally such as Gmail, without prior notice or permission from the account owner. As such, students and staff have no expectation of confidentiality or privacy with respect to any communication or access made through District systems and network or on District-issued computers, regardless of whether that use is for District-related or personal purposes, other than as specifically provided by law. The District may, without prior notice or consent, log, supervise, access, monitor, view or record the use of District systems and network (including reviewing files and other materials) at any time. By using or accessing District technology, all students agree to such access, monitoring and/or recording of their use.