DODGELAND SCHOOL DISTRICT
Board Policy Manual

363.2 - Rule

STUDENT TECHNOLOGY USE GUIDELINES

A. Network Guidelines

The following standards will help to ensure the safe, efficient use of the District's technology network.

Student technology network use that is considered unacceptable and prohibited at all times includes, but is not limited to:

- use for private or commercial business purposes.
- use for political, or religious purposes.
- any illegal activity, or other action that violates any other Board policy.
- accessing inappropriate materials, including sexually explicit, obscene or pornographic items, and other materials considered harmful to minors.
- sending material likely to be offensive or objectionable to recipients.
- sending messages or taking other actions that harass or bully others.
- using programs that infiltrate the network system to damage the software components or destroy data.

Student technology network use that is considered acceptable and is expected of responsible users includes, but is not limited to:

- making the most efficient use of network resources to minimize interference with others.
- when the network is used to access outside resources, conforming to technology use policies and procedures of both this District and the other district or entity that possesses the outside resources.
- obtaining pre-approval by the District for subscriptions to Listservs, bulletin boards and other on-line services, and avoiding use of such services when approval is denied.
- obtaining authorization from the IT Department prior to connecting personal technology equipment (e.g., electronic devices, printers, wireless devices, switches, routers, hubs, etc.) to the District network.
- obtaining approval of the IT Department prior to installing or downloading software.

The District limits the amount of available network storage to students. Some files must not be stored on the network servers unless directed by an authorized teacher, administrator or IT Administrator. Unauthorized items or files shall be deleted when identified including, but not limited to, movies, music and personal pictures.

1. Network Security Guidelines

Security is a high priority in the District, especially when the network involves many users. Users are expected to follow responsible security measures including, but not limited to:

- notifying a teacher or other staff member immediately if a security problem on the network is identified.
- not demonstrating the security problem to other network users.
- not attempting to log onto the network as a system operator or administrator.
- respecting the rights and property of others, and not improperly accessing, misappropriating or misusing the files, data, or information of others.
- not sharing accounts with anyone, or leaving the account open or unattended
- keeping all accounts, user IDs and passwords confidential, and not accessible to others.
- making back-up copies of the documents that are considered critical.
- taking precautions to prevent viruses on District and personal technology equipment.

Users identified as a security risk, or having a history of problems with the DSD network or equipment, shall be denied access to the network, and may be subject to disciplinary and/or legal action.

2. Internet Guidelines
When using Internet interactive, social networking and other special sites or services, users are subject to all of the technology use policy provisions and regulations that apply to the use of District technology equipment and the network. Additional regulations that apply to Internet use include, but are not limited to, the following:

- Certain Web 2.0 Services such as Moodle, wikis, podcasts, RSS Feeds and blogs that emphasize online educational materials and sharing among users may be permitted by the District with prior approval of the teacher, principal and IT Department.
- Facebook, MySpace, YouTube, and other social networking sites are prohibited unless given permission by an administrator or the IT Department. Students in specialized classes may also use these social networking tools if properly authorized by the teacher, principal, and IT Department.
- Streaming media, downloading media, and playing online games on District technology equipment or the network are prohibited unless authorized by the teacher, principal, and IT Administrator for educational purposes related to classroom instruction.

3. E-mail Guidelines
When using District e-mail accounts, users are subject to all of the technology use policy provisions and regulations that apply to the use of District technology equipment and the network. Additional regulations that apply to e-mail use include, but are not limited to, the following:

- Students may access personal e-mail accounts only before and after school unless authorized for specific educational purposes.
- Notification should be made to the sender if a message received was intended for someone else.
- District e-mail use shall be restricted to authorized educational purposes.
- District e-mail use for chain mail, solicitations, and advertisements is prohibited.
- Improper messages or use shall be reported to a teacher, principal or the IT Department.

B. <u>Electronic Devices</u>

When using school-owned/issued electronic devices, or personal electronic devices that are connected to District equipment, users are subject to all technology use policy provisions and regulations that apply to the use of District technology equipment and the network. Additional regulations that apply to electronic devices include, but are not limited to, the following:

- Students shall only use school-owned/issued electronic devices for instructional purposes during school hours. Such devices shall be the property of the district and may be copied, reviewed, and audited as deemed necessary by the District. Exceptions for the use of personal devices may be approved by the building principal.
- Students may use personal electronic devices before and after school hours.
- Students shall not connect personal electronic devices to any District technology equipment (e.g., camera, USB external drive, etc.) unless authorized by a classroom teacher. Students may be allowed to connect personal devices to the district public wi-fi.
- Students shall never use any school-owned or personal electronic device that can be used to capture, record or transfer images in private designated areas including locker rooms and bathrooms.

C. <u>Penalties/Consequences for Violations</u>

Violations may result in a loss of access, other disciplinary action and/or legal action based on the discretion of administration in accordance with legal requirements, district policy and established procedures.

Minor first offenses may be subject to a warning or advisory disciplinary referral. More serious offenses and/or repeated offenses shall be subject to loss of access, and may be subject to other disciplinary action or legal action for criminal offenses.

Loss of access may include the revocation of network privileges, including the Internet and/or e-mail. The duration of the specified privilege loss shall be determined based on the type and severity of the violation, and shall be based on the following guidelines:

- 1st offense — 4 weeks
- 2nd offense — 8 weeks
- 3rd offense — 12 weeks
- 4th offense — 16 weeks
- 5th offense — Remainder of student career at designated level

The designated career levels are defined by the following grade spans:

- Grades Pre-K – 5,
- Grades 6 - 8, and
- Grades 9 - 12.

If a personal electronic device is used in violation of District policy or rule, the device shall be confiscated and the user subject to disciplinary action. Conditioned on the type and severity of the violation, and the type of device, the following guidelines apply:

- First violation - the user of the device will receive an advisory disciplinary referral and the owner may pick up the device from the principal after 3:00 p.m.
- Subsequent Violations - A disciplinary referral will be made and the parent/guardian of the user will be required to pick up the device from the principal.
- Violations Involving Devises Potentially Harmful – Devices that could cause bodily harm (e.g. zappers, laser lights) are prohibited on school premises and at school related activities at anytime. Violations shall result in disciplinary action.

Revised (WASB): July 26, 2010
Revised: October 26, 2015