DODGELAND SCHOOL DISTRICT
Board Policy Manual

522.7 - Rule

STAFF TECHNOLOGY USE GUIDELINES

A. Network Guidelines

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

Staff 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.
- installing or downloading software for school or professional use.

Staff 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.
- 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.

The District limits the amount of available network storage to staff members. Some files must not be stored on the network servers unless directed by an authorized 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 an IT Administrator 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.
- not using another person's account or other network accounts without an IT Administrator's authorization.
- keeping all accounts, user IDs and passwords confidential, and not accessible to others.
- making back-up copies of the documents that are considered critical.
- securing computers and other technology equipment by logging off from systems or providing physical security when leaving the vicinity of the equipment.

- not using the District network for online banking, purchases or other purposes that require the sharing of personal information.
- taking precautions to prevent viruses on District and personal technology equipment.

The District shall not be liable for any personal information lost or stolen as a result of inappropriate personal use of the District network. 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 principal and IT Department.
- Facebook, Twitter, YouTube, and other social networking sites are prohibited unless given permission by an administrator or the IT Department. Staff teaching specialized classes may also use these social networking tools if properly authorized by the principal, and IT Department.
- As representatives of the District, social networking with students is discouraged unless there is a direct connection to educational purposes.
- Streaming media and downloading media on District technology equipment or the network during school hours are prohibited unless such activities are related to classroom instruction.
- Playing online games on District technology equipment or the network is prohibited unless authorized by an IT Administrator.

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:

- Staff shall check e-mail daily.
- District e-mail use shall be restricted to authorized educational purposes and school business.
- Limited personal use is allowed if staff members conform to school etiquette standards.
- Messages kept in the electronic mailbox should be kept to a minimum.
- Unwanted messages should be deleted immediately and messages from unknown senders should not be opened.
- Notification should be made to the sender if a message received was intended for someone else.
- District e-mail use for chain mail, solicitations, and advertisements is prohibited.
- Improper messages or use shall be reported to a principal or the IT Department.
- Staff shall be aware that, based on court cases, e-mail documents may be considered legally binding.

4. Web Page Guidelines

When creating and managing school Web sites, staff members 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 school Web sites or pages include, but are not limited to, the following:

- School Web sites shall be via the District's Web hosting service.
- The District has the right to approve any pages that are linked to the District Web site.
- The first and/or last name of a student shall only be published on a Web page with written parent/guardian permission.

- Student Web pages shall be clearly identified and contain a disclaimer that student opinions do not necessarily represent the District.
- The home page of each school Web site shall contain a copyright notice.
- Web sites shall not contain copyrighted material without obtaining proper permission.
- The staff member creating a Web page is responsible for the content of the page, including the links.
- Links shall be created between the District home page and each school Web site.
- Links must only contain materials and information that are related to educational purposes and align with District policies and procedures.
- Curriculum connections shall be linked to the District curriculum standards.
- Other links shall be only be made to sites that provide information about youth activities, agencies or organizations. Such activities, agencies or organizations must be non-sectarian, nondiscriminatory and committed to school-community interests such as child welfare.

5. Student Information System

When using the Student Information System (SIS), 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 the SIS include, but are not limited to, the following:

- The SIS and messages transmitted and documents created on the system are property of the District and supervised by the District.
- Access to the SIS requires authorization of the IT Director.
- Information contained in the SIS, or related to the system, shall be shared and/or disclosed only by staff members specifically authorized to disclose such information and only in accordance with legal requirements, and District policies/procedures related student records.

B. <u>Electronic Devices</u>

When using school-owned 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:

- Staff members are encouraged to only use school-owned electronic devices during school hours or activities unless approved by an IT Administrator.
- Such devices shall be the property of the district and may be copied, reviewed, and audited as deemed necessary by the District.
- Staff shall not connect personal electronic devices to the private District network or technology equipment.
- Staff 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.

Revised (WASB): July 26, 2010
Revised: October 24, 2016