

ACCEPTABLE INTERNET USE

The Dickinson School District believes ~~Internet network~~ access plays an important role in the education of students; however, the ~~Internet network~~ also contains content that is not appropriate for students and staff ~~to access~~. ~~In accordance with federal law, the~~ The District has taken reasonable precautions, ~~accordance with federal law,~~ to restrict ~~students and staff~~ access to ~~materials~~ obscene, pornographic, and/or harmful ~~to minors~~ ~~information~~ through the use of software designed to block sites containing inappropriate material. While the District has taken ~~such~~ preventive measures, it recognizes that it is not possible to fully guarantee that students and/or staff will never access objectionable materials.

Education

The District shall provide education to students ~~and staff~~ about appropriate online behavior, including interacting with other individuals on social networking websites ~~and in chat rooms,~~ ~~as well as~~ ~~and~~ cyberbullying awareness and response.

Students bringing personal technology to school including, but not limited to, cell phones, tablets, laptops, and handheld games, must adhere to the Student Use of Personal Technology Policy (FFI), classroom and/or building rules related to personal technology use, and all other applicable student conduct policies.

Monitoring Use

~~Internet Network~~ access is a privilege, not a right. Network storage areas shall be subject to the same scrutiny as school lockers for students. ~~Students and staff~~ shall have no ~~reasonable~~ expectations of privacy when using district computers and/or networks and shall use this technology solely for ~~work-related classroom/district-related~~ purposes. Network administrators may view files and communications to maintain the integrity of the system and to ensure proper and responsible use of the system. Teachers and administrators will exercise supervision of student use.

Prohibitions

The District subscribes to the acceptable use policies of EduTech. All district computer users shall abide by this policy. The Superintendent or designee may take disciplinary measures when any of the following actions occur:

1. ~~Accessing, downloading, or publishing or creating pornographic files or sites and/or other~~ inappropriate internet material;
2. ~~Sending or posting threatening, harassing, insulting, annoying or alarming content; Harassing, insulting, threatening, alarming, or attacking others;~~
3. ~~Sending, posting, or using~~ obscene language;
4. ~~Violating the privacy rights of students and employees of the District;~~
5. ~~Vandalizing and/or tampering with District computers and/or networks; Damaging computers, computer systems, or computer networks;~~
6. ~~Hacking or any other form of unauthorized access to accounts, computer systems, or files;~~
7. ~~Attempting to breach network security or transmit viruses;~~
8. ~~Violating copyright, trademark, trade secret, or other intellectual property laws;~~
9. ~~Using or participating in chat lines, chat rooms, and social networking sites for personal and/or non-curricular purposes;~~
10. ~~Accessing social networking or other internet sites for noncurricular purposes;~~

REQUIRED

Descriptor Code: ACDA

11. Using another's password or representing oneself as another;
12. Trespassing into another's folders, work, or files;
13. ~~Intentionally wasting network resources, including, but not limited to, emailing chain letters and/or broadcasting inappropriate messages;~~
14. ~~Employing~~ Utilizing the network for political purposes as defined by state law, financial gain and/or commercial purposes;
15. ~~Revealing anyone's personal information, such as, but not limited to, an address or phone number without appropriate consent. Students are prohibited from revealing personal information about themselves and/or others without obtaining written consent in accordance with the Federal Education Rights and Privacy Act and receiving administrative approval;~~
16. Other ~~activities or~~ actions deemed inappropriate ~~and or is~~ not in the best interest of the District, its employees, and students.

Violations

~~Violation of this policy will, at a minimum, result in the following disciplinary consequences for students:~~

- ~~1. First offense (Level I)
 - a. Loss of SENDIT/email and Internet privileges for four weeks;
 - b. Parents contacted.~~
- ~~2. Second offense (Level II)
 - a. Loss of SENDIT/email and Internet privileges for at least the remainder of the year.
 - b. Parents contacted.~~
- ~~3. A student may be subject to Level II disciplinary action and/or other appropriate disciplinary measures on his/her first offense if administration deems this necessary based on the severity of the offense.~~

~~Violations of this policy, or any federal/state law, rule or regulation, may result in loss of network privileges, as well as further disciplinary action up to and including suspension or expulsion for students or termination of employment for staff, as determined by the Superintendent or designee. Violations of this acceptable use policy or any applicable federal or state law, rule, or regulation may also result in disciplinary action up to and including expulsion for students or termination of employment for staff.~~

Consent

~~All students and staff must consent to this policy in writing prior to accessing District networks, computers, and/or other technologies.~~

Complementary Documents

- ABCA, Copyrighted Material and Intellectual Property
- ~~FF, Student Conduct and Discipline~~
- ~~FF-AR, Student Conduct Standards and Disciplinary Procedures~~
- FFI, Student Use of Personal Technology
- FFI-AR, Use of Technology in the Classroom
- FFI-E, Personal Technology Use and Waiver of Liability
- FFK, Suspension and Expulsion
- FFK-BR1, Suspension and Expulsion Regulations

REQUIRED

Descriptor Code: ACDA

- FGA, Student Education Records and Privacy
- FGCA, Searches of Lockers

End of Dickinson School District #1 Policy ACDA Amended: 05/08/17