STUDENT ACCEPTABLE TECHNOLOGY USE

The School District of Grafton is committed to free and open inquiry and discussion, fair allocation of District resources, and the provision for an educational environment free of needless disruption. Technology resources, computers, presentation equipment, network resources, communication systems, and Internet access (herein known as the Network) are available to all students (users) at the District for the purpose of supporting the educational mission of the District.

Acceptable Use

The Network is to be used only by persons authorized by the District and only for appropriate purposes. Each user shall take full responsibility for his or her use of the Network, including all messages, data, images, files, video, audio, and text that they access or transmit through the Network, regardless of whether that use of the Network is on-site or from off-site (non-District) locations. Users shall use social networking sites, chat, e-mail, blogs, wikis, web content publishing, or other shared online communication tools appropriately.

The District expects all users using the Network to exercise good judgment designed to further the student's education with the District. Examples of use that is not appropriate and does not demonstrate good judgment includes but is not limited to use, including accessing or transmitting content that is:

- pornographic or obscene (for example, U.S. Code 18 Chapter 71 Section 1468)
- child pornography (for example, U.S. Code 18 Section 2256)
- harmful to minors as identified in the Children's Internet Protection Act (CIPA)
- derogatory, threatening, violent, or discriminatory, and accessed or transmitted without legitimate educational purpose such as research
- in violation of the District Harassment/Intimidation Policy (411.1)
- in violation of the School Bullying Policy (443.75) (cyber bullying)
- in violation of Equal Educational Opportunities Policy (411)
- for impersonating the identity of another individual (including identity theft)
- attempting to falsify an online identity
- attempting to share personally identifiable information with any person or website unless authorized by the District
- an invasion of the privacy of others
- for private financial gain
- inconsistent with the requirements of any applicable license, copyright, or other contractual or legal protection of that content
- in violation of any school rule, District policy, state or federal law

If a user finds that he or she is using, transmitting or accessing content that contains material that is not appropriate including but not limited to those listed above, then he or she must

immediately terminate that use, which may include disconnecting from the website, regardless of whether that content has been previously deemed acceptable by any technology protection measure. The user must inform the teacher or supervisor of the incident.

Internet Safety

The District uses software designed to filter and block access to pornographic Internet sites. The District uses commercially reasonable technology protection measures designed to comply with CIPA's requirements. The District may also block sites that are recommended for blocking by the Superintendent or the Superintendent's designee. In certain limited circumstances reserved to the discretion and decision of the Superintendent or the Superintendent's designee, the technology protection measures may be disabled, circumvented, or minimized for those demonstrating a bona fide research need to access such filtered or blocked materials, or for other lawful purposes.

User Accounts

Authorized users will be provided a username and password to access the Network.

Kindergarten and Early Childhood students will be granted generic user accounts without a password.

Authorized users of technology are responsible for the use of their individual user account and files.

No user shall share a personal user account password with another user, nor obtain another user's account password by any unauthorized means.

No user without specific authorization by the District shall read, alter, or delete any other user's computer files or electronic messaging, even if the operating system of the computer permits them to do so.

Systems Management, Security, Monitoring, and Data Integrity

No District User should have any expectation of privacy as to his or her use of the Network, including any use of computers or Internet usage, or the privacy of any content in communications, electronic mail messages, files, searches, downloads, notes, or other data stored on, transmitted, or received through the Network. The District reserves its right to monitor and record use of the Network, including Internet usage.

The District, through appropriate management personnel, reserves the right to inspect any and all data stored on the Network and any personal storage systems of any kind used on the Network, without notice or warning, and at any time or for any purpose.

No user may use the Network to use, download, or distribute software or data that is not authorized by the District, including any pirated software, or software used in a manner inconsistent with its license agreement or applicable copyright law and District Use of Copyrighted Materials Policy and Rule (771.1, 771.1 Rule). Any use or content created or transmitted using the Network becomes the property of the District, subject to the restrictions of any existing licensing agreement or applicable copyright law or policy. Software, downloads, and other content may only be used in a manner consistent with their licenses or copyrights and applicable District policy and other controlling laws.

No software should be installed that is not directly authorized by the District. Users should seek the assistance of qualified systems management personnel in using non-standard software and data, and must never install downloaded software to networked storage devices without the assistance and approval of appropriate personnel.

No user may use the District's Network and/or computing facilities to propagate any virus, worm, Trojan horse, trap-door program code, root kit, or any form of destructive or malicious hardware or software instruction. Users may not propagate any virus "warnings" via network communication except to alert appropriate District systems management personnel. The District does use anti-virus software designed to protect the Network.

No user may intentionally delete or modify data that is used as part of an approved educational curriculum, except where the deletion or modification of said data is part of that curriculum.

No user may use the Network to disable or overload the Network, any property of the District, or any system on the Internet, or to circumvent any system intended to protect the privacy or security.

No user shall waste shared resources such as disk space, network bandwidth, printer paper, or printer toner. Users must be efficient in their use of these resources.

No user may physically tamper, move, alter, or dismantle any property, including software, unless authorized by the District.

No user may use the Network to access or attempt to access stored materials or data that are not appropriate for the user's legitimate intended use.

The District reserves the right to determine which content is kept, modified, or destroyed in accordance with District policy, state and federal law.

The District makes no warranties of any kind, whether expressed or implied, for the services it is providing. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services, including the Internet. The District will not be

responsible for any damages a user may suffer, including but not limited to, loss of data or interruptions of service.

Enforcement

Failure to comply with this policy will result in the student being disciplined by the building administrator in accordance with building rules and the Student Discipline Policy (447), restrictions on use, and other corrective action determined by the District.

The District reserves its right to cooperate with requests from law enforcement and regulatory agencies for information regarding individual use of the Network.

The District shall not discriminate in the selection and evaluation of textbooks or related materials on the basis of sex, race, color, religion, national origin, homeless status, ancestry, creed, pregnancy, marital or parental status, sexual orientation or physical, mental, emotional, or learning disability or handicap or any other reason prohibited by state or federal law.

Legal Ref: Wisconsin State Statutes Sections 120.13 (1); 121.02 (1)(h); 943.70; 947.0125;
Copyright Law of the United States of America, Pub.L.No.94-553,90 Stat.2541.
(U.S. Code 18 Chapter 71 Section 1468)
PL 106-554 Children's Internet Protection Act (CIPA)
Equal Educational Opportunities Policy (411)
Student Harassment/Intimidation Complaint Reporting Procedures Policy (411.1)
School Bullying Policy (443.75)
Student Discipline Policy (447)
District Use of Copyrighted Materials Policy and Rule (771.1, 771.1 Rule)

Revised: June 5, 2000
Approved: July 17, 2000

Date of First Reading: November 15, 2010
Date of Second Reading: November 22, 2010
Revised: November 22, 2010