IIBGA

School District of Bonduel
Technology Acceptable Use
&
Internet Safety Policy (TAUP)

This policy covers all employees, students, and other users of District technology.

Students agree to adhere to this policy by signing handbook agreements. Employees agree to follow this policy by signing the School District of Bonduel Employee Handbook. All other users must either fill out a technology account application with the Director of Technology or agree to terms in the policy by accepting terms on agreement screen prior to accessing the District network.

The School District of Bonduel is proud of its status as a leader in technology implementation and education. The District offers vast, diverse, and unique resources to students, staff, and community members. The District's goal in providing these services is to promote educational excellence by facilitating resource sharing, innovation, and communication.

Technology Defined

The use of technology, which is defined under this policy as including, but not limited to the use of software, audio and video media, computers (desktops, laptops, tablets, etc.) and hardware peripherals or external devices, network and telecommunications equipment, and video and audio equipment owned or leased by the School District of Bonduel. This policy also governs use of any and all technology used to access network resources (remote access to the network, personal devices used on District owned or leased network resources, personally owned devices using district software), are subject to the terms of this policy.

Purpose

The School District of Bonduel realizes the importance of incorporating technology and the vast resources of the Internet to enhance the curriculum. The District recognizes that as telecommunications and other new technologies shift the ways that information may be accessed, communicated, and transferred by members of society, those changes may also alter instruction and student learning. The District supports access by students and staff to rich information resources along with the development of appropriate skills to analyze and evaluate resources. In today's world, access to and manipulation of information is a critical skill. Staff and students will have available to them age/grade appropriate technological tools necessary to explore the world both from inside and outside the classroom walls.

General Responsibilities

The School District of Bonduel has the capability to monitor use of network resources. Users should not expect that files, data, e-mail, external devices connected to the District network or any other resources stored on or used to connect to district servers or other hardware will be private or confidential.

With these learning tools, all users must understand and practice proper ethical use and security. Use of technology, including the Internet, is a privilege, not a right, which may be revoked at any time for inappropriate conduct.

Internet safety must be exercised at all times by all users. According to the *Children's Internet Protection Act* (CIPA) of 2000, this policy must address:

- Access by minors to inappropriate material on the Internet and World Wide Web
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications (i.e. Instant message services, blogs, wiki's, podcasts, IP telephony programs)
- Unauthorized access, including so-called "hacking" and other unlawful activities by minors online
- Unauthorized disclosure, use, and dissemination of personal identification information regarding minors
- Measures designed to restrict minors' access to materials harmful to minors

On October 10, 2008 congress passed S. 1492: Broadband Data Improvement Act (iii) which requires elementary and secondary schools with computer access to the Internet to educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

The School District of Bonduel will make reasonable efforts to block, filter and monitor access to visual depictions that are obscene, child pornography, harmful to minors, or that the School District of Bonduel determines is inappropriate for minors.

All users (students and adults) are required to report any sites that contain inappropriate materials or materials harmful to minors. This information is to be reported by a student to the supervisor in charge or if a staff member, to the District Technology Director. This would include any text, audio segment, picture, image, graphic image file, or other visual depiction that--

- Takes as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion
- Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated or perverted sexual acts, or a lewd exhibition of the genitals
- Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

It is the responsibility of all instructors/employees to properly inform students/staff under their charge of this policy and to see that the policy is strictly enforced.

Acceptable Uses:

Examples of appropriate conduct include but are not limited to:

- Use consistent with the mission of the School District of Bonduel
- Use of technology, including the Internet, for Board approved curriculum-related activities
- Use that encourages efficient, cooperative and creative methods to perform the user's job duties or educational tasks
- Use in support of research and education

- To provide unique resources to and collaborative projects with Board approved educational partners or administrator approval.
- Use to communicate with and between students, staff, parents, and other stakeholders to support and enhance the learning environment
- Use only accounts, usernames, and passwords that are assigned to you
- Your right to free speech applies to your communication on the Internet. The District Network and all related resources are considered a limited forum, similar to the school newspaper, and therefore the District may lawfully restrict your speech for valid educational reasons. This includes school provided email accounts.
- Use of district-approved external storage devices (digital lockers, flash drives, etc.) for curriculum-related electronic information transfers (documents, images, video, etc.)
- All other uses must be approved by the administrator in charge, if an employee; or the teacher in charge, if a student

Unacceptable Uses:

Examples of inappropriate conduct include but are not limited to:

- Use of personal or District owned or leased technology, including the Internet, for anything but Board approved curriculum-related activities or other approved uses.
- Use of technology for a commercial, political, or profit making enterprise, except as specifically agreed to with the District
- Accessing or distributing inappropriate material (i.e. obscene, abusive, threatening, harassing (religious, sexual, racial), or any material specifically prohibited by federal, state, or local law)
- Send, display, or store (on district servers or district-provided digital storage) offensive messages or pictures, pornography, email, etc.
- Use obscene language
- Use of technology to harass, bully, insult, or attack others
- Use of the Internet for unlawful or malicious activities
- Intentionally attempting to or successfully bypassing filtering software while using District technology or the District's network
- Breaching security by sharing and/or using unauthorized passwords or working from network or web-based accounts not assigned to you
- Activities that could cause congestion and disruption of networks and systems
- Deliberate destruction or diminishment in value or effectiveness of any technology system or information. Any cost to repair deliberately damaged technology will be the responsibility of those causing the damage
- Attempt to illegally access, alter, or delete files, data, information, or accounts
- Misrepresentation of oneself; attempting to gain unauthorized access including attempting to log in through another person's account or access another person's files
- Use of unauthorized software, hardware, printers, using district technology or printing non-school-related materials using District technology
- Behavior in violation of district policy or regulations, copyright laws, state statutes, or federal laws
- Student users will not post personal contact information about themselves or others on the Internet or World Wide Web including: last name, address, e-mail address, telephone number, social security number, personal photograph

- Load software, programs or other media on District owned hardware

If you are not sure if an action is permissible, contact a teacher or supervisor for clarification.

Additional User Responsibilities:

- All users will promptly disclose to their teacher or supervisor any network communication they receive that is inappropriate or makes them feel uncomfortable
- All users are responsible for the activity recorded to their network accounts and bear responsibility for actions that occurred as a result of sharing of account information
- All users are responsible for notifying the staff member in charge who must then report to the Director of Technology when they believe a breach of security or other violation of this policy has occurred

Additional Considerations for Technology Use Beyond School Buildings:

- This policy covers use of all district technology both on and off of school grounds
- Filtering and monitoring software can be installed on District owned technology and activity off-site is subject to this filtering and monitoring
- While filtering software may be installed on District owned technology, no filter provides the level of supervision an adult can provide. Parent(s)/guardian(s) should always monitor minor students using technology
- While this policy does not cover privately owned technology used off-campus, users should be aware that cyberbullying and other inappropriate activities conducted off school grounds using private technology can still be consequenced at school if they create a substantial disturbance at school

Consequences:

Student User violations will be handled by building administrators in accordance with school disciplinary procedures identified in the student handbooks. Policy violations can result in action up to and including limitations or revocation of technology privileges, suspension, and even expulsion. In all cases, restitution for intentional damages will be assessed.

Employee violations of the TAUP policy will be handled in accordance with the disciplinary procedures identified in the collective bargaining agreements. Policy violation may result in appropriate disciplinary action up to and including written reprimand, suspension without pay, and possible discharge.

The District Administrator will issue and review penalties regarding employee violations. In all cases, restitution for damages will be assessed.

Approved:	5-18-98
Revised:	5-19-99
	4-17-2000
	4-2-2001
	1-2-2007
	1-7-2008
	7-6-2009
	8-20-2012