

Technology Acceptable Use Policy for Staff and Students

(Adopted 7-18-2016)

TECHNOLOGY VISION STATEMENT

It is the vision of the Jamestown School District to maximize learning for students through the use of current technology. By including technology in our K-12 curriculum, we can continue to instruct students in the basics, promote self-worth, promote active student-centered learning, and equip students with present and future skills. The use of technology as a tool improves the ability of students, teachers, administrators, and the entire community to gather, use, and distribute information more efficiently and more effectively.

POLICY

The Jamestown School District's technology resources shall be used for educational purposes consistent with the district's mission and goals, district policies, state laws, and federal laws. The Jamestown Board of Education will provide the opportunity and the training for staff to appropriately use the district's technology resources.

Staff and Student ("users") use of technology resources that include but are not limited to:

- Computers and related peripherals (including printers, portable hard drives/USB/flash drives, mp3 players, etc.)
- Personal Learning Devices (including iPads, Nooks, Kindles, etc.)
- Networks including local, cloud based, and cellular.
- Local and wide area networks, including wireless networks
- File and application servers both onsite and offsite
- Video networks, digital video camcorders, and cameras
- Telephones, voice mail systems, cell phones, smart phones PDAs, fax, and copy machines
- Televisions, projectors and other audiovisual equipment. VCRs, DVDs, laserdisc players, etc.
- Printers of all types
- Internet access
- Office 365 Suite including Outlook, One Drive, Word, Excel, PowerPoint, Sway, Video, Delve, Calendar and more including access to Internet web building.
- IVN or interactive learning
- SMARTBoard and SMART technologies.

Use of these technologies must be consistent with academic actions of the Jamestown Public Schools (JPS). Users are expected to adhere to the district policies as they apply to district and personal technology resources. Users are also required to comply with all local, state, and federal laws, which include regulations against computer/network hacking, software piracy, copyright infringement, bullying and other illegal behaviors.

JPS prohibits technology uses, whether with district or personal technology used on district property, which could injure a person either physically or emotionally. Prohibited uses include, but are not limited to:

- Bullying or harassing others
- Use of the network for product advertisement or political lobbying.
- Sending or displaying offensive messages or pictures, including pornography.
- Students taking pictures of others and sharing publicly any photo without that person's permission or knowledge
- Use of the network for hate mail, discriminatory remarks, and offensive or inflammatory communication.
- Using obscene language.
- Harassing, insulting or attacking others.
- Damaging computers, computer systems or computer networks.
- Violating copyright laws including plagiarizing, downloading or exchanging pirated software, music, or other files.
- Use others' passwords, tampering with or forging names on electronic mail or other online environments.

- Trespassing in others' folders, work or files.
- Using another person's identity or falsifying your own within any digital correspondence or online persona.
- Any action hacking with intent to damage or for the purposes of circumventing standard technology configurations or policies.
- Loading or use of unauthorized games, programs, files, or other electronic media.
- Intentionally wasting network resources.
- Storage of games and excessive picture, music, and video files.
- Unauthorized posting of personal information about others, including phone numbers, names, etc.
- Performing any action that results in a compromise of the system security.
- Inappropriate use of personal handheld electronic devices, including cell phones.
- Using the network for any illegal, unethical, or commercial activities.
- Negligent release of confidential data.

Employee technology use, that is not specific to one's job duties, is acceptable under the conditions that it does not:

- interfere with the performance of that employee's duties.
- create the appearance of impropriety.
- result in political or personal commercial purposes.
- increase operational costs for the district.

1:1 Devices

The Jamestown Public School District is cognizant that students and staff may be using personal technology resources in the school environment. Examples are cell phones, PDAs, laptops, iPads, tablets, etc. The use of personal technology resources not owned by the school falls under the Technology Acceptable Use Policy. The school is not responsible for the loss of items with significant personal or financial value. School administrators shall use their discretion to determine a building policy for personal technology resources used in the school that may not be specifically addressed in this document.

Jamestown Public School District staff, students and parents/guardians fully acknowledge that the use of a personal device on the premises of JPS is subject to all guidelines, rules, and regulations governing responsible use as established by the Jamestown Public Schools. It is further understood that the use of a personal device is restricted to those activities as required or related to the student's program of study and any other use may be subject to disciplinary action including the loss of device use privileges. Students will not access websites with inappropriate content using a 3G or 4G connection.

By logging on to the JPS wireless guest network, staff and students are accepting the terms of the JPS Technology Use Policy. The JPS wireless network will provide filtered Internet access just like the network for JPS devices.

Electronic Communication

Electronic communication between staff and students should always be Transparent, Accessible, and Professional (TAP) as defined below:

1. The communication is **TRANSPARENT**: All digital communication between staff and students should be transparent. As a public school district, we expect to maintain openness, visibility, and accountability with regards to all communications.
2. The communication is **ACCESSIBLE**: All digital communication between staff and students, shall be considered a matter of record, part of the District archives, and/or may be accessible by others.
3. The communication is **PROFESSIONAL**: All digital communication from staff to students should be written as a professional representing the Jamestown Public School District. This includes word choice, tone, grammar, and subject matter that model the standards, and integrity of the profession.

Communication Methods

1. Acceptable Methods of communication between staff and students.
 - a. School Website – www.Jamestown.k12.nd.us and other web sites or portals endorsed by the district.
 - b. Jamestown Public School Google Domain
 - c. PowerSchool, ParentLink-Teacher Connect or Edmodo
 - d. One-way or Two-way Messaging – Internet service sending text to registered individuals to receive notifications. The preferred method of communication for school district personnel is the district's calling/texting service (ParentLink-Teacher Connect).
 - e. Two-way Messaging – Not encouraged. If two-way texting is necessary, Jamestown School District personnel must follow TAP guidelines, and he/she must have parental permission prior to using two-way texting.
2. Unacceptable Methods
 - a. Non-District Email Accounts – Jamestown School personnel should never use personal email accounts to communicate with students about school matters. Coaches may obtain a school district email account and must also follow these expectations.
 - b. Coaches will be provided with a ParentLink Teacher Connect account and will need to create groups to make contact with players and/or parents.
 - c. Online Games and Related Activities – While many people enjoy gaming (Wii, Xbox, etc.) and recreational websites that allow them to compete with others through the Internet, this is not an acceptable activity for school personnel to engage in with students.

Social Media

General Guidelines

Staff members who are using social media should be cautious in the communication with these technologies. Comments or posts placed on these sites can be visible by a large audience including parents and students. Staff members should never “friend” students who are currently enrolled in Jamestown Public School. The separation between the role of a public educator and a personal friendship with students should always be visible and strongly communicated.

Any content staff members publish, pictures they post, or dialogue they maintain within any social media, or blog, should never compromise their professional integrity or ethics in their role as a professional employed by Jamestown Public School.

Personnel are not authorized to speak on behalf of the district in an official capacity, without prior consent by the Administration. Any opinions or comments about the district and related programs should clearly acknowledge that the comments are their personal opinions and not reflect the opinions of the district.

1. Facebook
 - a. The Jamestown Public School uses Facebook as a means to communicate with students, personnel, and patrons. Facebook can be a valuable tool to communicate with others and its use by school personnel is NOT prohibited.
 - b. If school personnel use Facebook for valid educational objectives in their classroom or student organization, the page should be set up as an Artist, Band or Public Figure Page, not a personal page. This allows all public to view the page and keep all content on it visible for all to monitor.
 - c. Communication with students within a Facebook Page should be centered on one-way communication. If two-way communication is used it should be monitored frequently by school personnel to ensure TAP guidelines are being followed. You can set your page up so that comments are not posted until you have reviewed them and this is recommended.
 - d. Any page created for educational purposes should be owned and monitored by Jamestown Public School personnel. If you wish to create a Facebook page to be used within your course or student group be sure to notify parents of your intent to communicate in this fashion.

2. Twitter

- a. JPS uses Twitter as a communication tool to share vital information and details to events held in the district.
- b. Any use of Twitter as a professional in the district to communicate with students and parents should be education focused and one-way.
- c. By establishing an account, it is your responsibility to monitor it closely.

Electronic Mail and Internet Use

- Users must adhere to this policy at all times when using the Internet and/or email, including after hours, weekend and/or holiday use.
- District email accounts will be provided to all employees and students grades five through twelve.
- Users are prohibited from using district or district provided (EduTech) email or Internet access for commercial or personal gain.
- Material hosted on district servers and published on the Internet may be reviewed for appropriateness. Materials that represent JPS and are hosted on non-district servers should adhere to this policy.
- Student email accounts will be provided through EduTech and will include the Office 365 Suite of software. Students are not allowed to access non-approved email accounts while in school. Student accounts may be revoked if used inappropriately as outlined in the EduTech Acceptable Use Policy or the Jamestown Public Schools Technology Acceptable Use Policy.

Office 365 Suite

Office 365 is a total Suite of tools. These tools continue to expand to even greater opportunities. Included with the Office 365 Suite are five free downloads for any student or staff with an @k12 account.

Collaborate with Office Online:

Mail	Calendar	People
Newsfeed	OneDrive	Sites
Tasks	Delve	Video
Word Online	Excel Online	PowerPoint Online
One Note Online	Sway	

Many instructors are using these in their classrooms so it is vital that staff, students and parents are aware of the impact inappropriate use of an @k12.nd.us account can have. If you risk having your account shut down due to violation of the District Technology Policy you could lose all features listed above and more that may be added in the future. This would also include the program downloads you have accessed at home. You would not be able to login to any portion of the program if it becomes necessary to lock your account. You also would not be able to login to a website if that was a class you were taking. This program through EduTech allows you have the tools you need to do your job in school and should be used wisely.

Internet Safety and Use of Filters

JPS participates in Internet filtering services provided through EduTech to help prevent access to Internet content that is obscene, pornographic, or harmful as defined by the Child Internet Protection Act. By default, filtering measures shall be in operation at all times during the use of the district's computers. Some filtering protection measures may be disabled by an authorized administrator, supervisor, or other authorized person in order to provide access to valid research or for other lawful purposes. In cases where JPS staff provide minimally filtered access to students, the teachers are expected to supervise students and can be held responsible for any student act that violates the Acceptable Use Policy. Problems with the filtering system should be reported immediately to the district Technology Department.

Although the district provides a filtering system to limit user access to potentially objectionable material, no filtering system can provide complete protection and it is the user's responsibility to access Internet resources appropriately.

Staff are responsible for supervising students using Internet resources.

Internet safety precautions are the responsibility of all users. Safety tips include:

- Keep your personal information (name, phone numbers, address, passwords, etc.) private.
- Do not read email or download attachments from people you don't know.
- Understand that nothing done on the Internet is private.
- Tell a trusted adult or supervisor if someone says things or sends you something that you consider inappropriate (do not respond to the person either directly or indirectly).
- Never meet online-only friends in person (you have no way to confirm the real identity of someone you meet online).
- Practice proper 'Netiquette' while online and avoid conflicts with other users.

Potentially objectionable material includes, but is not limited to:

- Visual depictions that are obscene or depict child pornography as defined by the Child Internet Protection Act.
- Violence/violent behavior
- Drugs/drug culture
- Cults/satanic
- Militant/Extremist
- Gambling
- Alcohol/tobacco/drugs
- Unrestricted email/chat

Privacy

Privacy is not guaranteed when using JPS technology, including the network. Files, communications (including email), and use history may be reviewed to maintain system integrity and ensure that users are adhering to the Acceptable Use Policy and guidelines. The district will cooperate with local, state, and federal authorities when necessary. All activity could fall under North Dakota open record laws, which means that someone can ask to review this information at any time.

Security

Network and computer security systems help maintain the integrity of the district technology resources. Any attempts to circumvent, disable, or misuse security systems are prohibited. If users feel they can identify a security problem they should notify the Technology Department.

Vandalism

Vandalism includes any malicious attempt to harm or destroy any JPS equipment or software or the data of another user on a computer, local network, or global network. Vandalism is prohibited and may result in cancellation of privileges or other disciplinary action.

Sanctions

The building administrator, supervisor, and/or teacher is responsible for applying sanctions when the Staff and Student Acceptable Use Policy has been violated. Possible sanctions include, but are not limited to:

- Loss of access to district or personal technology resources.
- Removal of students from classes with loss of credit.
- Suspension
- Termination of employment.
- Expulsion
- Restitution for costs associated with repair of equipment or software or associated with improper use of district equipment or systems.
- Additional disciplinary action may be determined at the site or district level in line with existing discipline

procedures.

- When applicable, law enforcement agencies may be involved.

Documentation of all violations of this Acceptable Use Policy may be placed in the employee's personnel file or the student academic file. Prior to the suspension/revocation of the use of technology resources or termination, the building administrator will inform the user of the suspected violation and give the user an opportunity to present an explanation. A system user may appeal the suspension or revocation within seven (7) calendar days to the superintendent.

Legal Disclaimer

JPS will not be responsible for damages users may suffer, including loss of data resulting from delay, non-delivery, or service interruptions; damages to personal property used to access school computers, networks, or on-line resources; or unauthorized financial obligations resulting from use of school accounts to access the Internet. JPS specifically denies any responsibility for the accuracy or quality of information obtained through Internet services.

Since all transactions conducted through district technology resources could be perceived as authorized district activities, users of district technology resources are responsible for respecting and adhering to local, state, federal and international laws. Any attempt to break those laws through the use of district technology resources may result in legal action against the offender by the district, injured third parties and/or governmental authorities. If such an event should occur, the district will fully comply with any requests for information related to the legal proceeding, subject only to prohibitions of law. The Jamestown Public Schools is not liable for the actions of users, which violate the conditions of this document.

The Jamestown Public Schools reserve the right to inspect, review, or delete contents if it has reasonable cause to suspect that a student is using technology for illicit or illegal purposes, is in violation of policy, or for general maintenance. School authorities may conduct such inspection when they deem it necessary, without notice, without consent, and without search warrant.