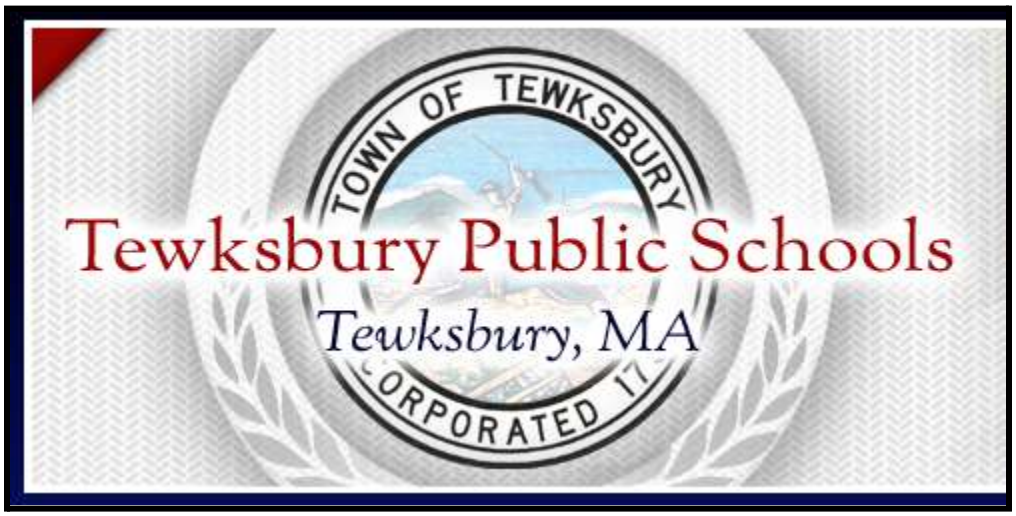

Technology Acceptable Use Procedures

(Pertaining to IJNDB and IJNDB-R – Acceptable Use Policy – Technology)

Tewksbury Public Schools
139 Pleasant Street
Tewksbury, Massachusetts 01876
(978) 640-7800
www.tewksbury.k12.ma.us

August 2023

Introduction

The Tewksbury Public Schools (TPS) recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, collaborate, and develop skills that will prepare them for work, life, and citizenship. Our goal is to promote educational excellence by encouraging and facilitating resource sharing, innovation, and communication. We are committed to helping students develop innovative/future-ready and communication skills. To that end, we provide the privilege of access to technologies for student and staff use.

Internet use that is integrated into the school curriculum fosters the development of research and information skills, encourages critical and higher level thinking, and provides expanded educational opportunities for both students and staff. While supporting the rights of students and staff to use all available tools, the Tewksbury Public Schools recognize that there is material on the internet that is objectionable or devoid of educational value within the context of a school setting. The Tewksbury Public Schools have taken steps to restrict access to inappropriate or controversial material as it relates to the educational goals of TPS. In addition to utilizing an internet content filter, TPS staff will closely supervise students' use of the internet.

Although guidelines cannot totally eliminate the possibility of inadvertent or intentional access to such information, we believe that they can significantly limit such possibilities. The Tewksbury Public Schools believe that the access to valuable resources on the Internet far outweighs the concerns that the users may procure material that is not consistent with the educational goals of the Tewksbury Public Schools, and we intend to maximize the Internet's educational value.

The Tewksbury Public Schools will insure that it adheres to the most recent Children's Internet Protection Act (CIPA) requirements of 2001 by:

- implementing an Internet filter for the purpose of blocking access to visual depictions deemed obscene, child pornography, or harmful to minors. It may be disabled for adults engaged in bona fide research or other lawful purposes.
- providing for educating minors (in this case 'minors' refer to school aged children up to the age of 17) about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response.

These Acceptable Use Procedures outlines the guidelines and behaviors that all users are expected to follow when using school technologies or when using personally owned devices on the school campus, or in Remote Learning from home including the following articulations of usage:

- The TPS network is intended for educational purposes.
- All activity over the network or using district technologies may be monitored and retained.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Users are expected to follow the same rules for good behavior and respectful conduct online as offline.

• Misuse of school resources can result in disciplinary action.
• TPS makes a reasonable effort to ensure users' safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
• Users of TPS network or other technologies are expected to alert IT staff immediately of any concerns for safety or security.

Technologies Covered

TPS may provide the privilege of Internet access, desktop computers, mobile computers or devices, video conferencing capabilities, online collaboration capabilities, message boards, email, and more. This Acceptable Use Procedure applies to school owned technology equipment utilizing the TPS network, the TPS Internet connection, and/or private networks/Internet connections accessed from school owned devices at any time. This Acceptable Use Procedure also applies to privately owned devices utilizing the TPS networks, the TPS Internet connection(s), and/or private networks/Internet connections while on or off school property. As new technologies emerge, TPS will seek to provide access to them. The policies outlined in this document cover all available technologies now and into the future, not just those specifically listed or currently available.

Usage

All technologies provided by TPS are intended for education purposes. All users are expected to use good judgment and to follow the specifics as well as the spirit of this document: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Web Access

TPS provides its users the privilege of access to the Internet, including web sites, resources, content, and online tools. Access to the Internet will be restricted as required to comply with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users are expected to respect the web filter as a safety precaution and shall not attempt to circumvent the web filter when browsing the Internet. The determination of whether Internet based material is appropriate or inappropriate is based on the content of the material, the materials rating/reputation, and the intended use of the material, not on whether a website has been filtered or not. If a user believes a site is unnecessarily filtered, the user should submit a request for website review to their building principal. Any attempt to circumvent Internet web filtering is not permitted and may result in disciplinary action which may include loss of Internet access privileges.

Computer and Email Accounts

An "account" typically consists of a username and password and is used to gain access to computer and cloud based resources, but isn't limited to this format. Using another individual's account or password is prohibited. Giving your username and password to others is prohibited. Tewksbury Public School Staff should not attempt to login to any system or resource as another user. Violation

will result in disciplinary action up to and including termination. Tewksbury Public School System students should not attempt to login to any system or resource as another user, doing so may result in cancellation of user privileges. Documents created utilizing these accounts should be for school purposes only. All documents are cr

Email

TPS may provide users with the privilege of email accounts for the purpose of school related communication and should not be used for personal or business activities. Availability and use may be restricted based on school policies. If users are provided with email accounts, the account(s) should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origins; should use appropriate language; and should only communicate with other people as allowed by TPS or the teacher. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and as a school department, all email communications are archived for seven (7) years.

Technology Specialists who operate the system have access to all mail, including deleted messages. Messages relating to or in support of illegal activities may be reported to the authorities. All communications and information accessible via the network should be considered public property; however, the use of another person's intellectual property without that individual's prior written approval or authorization is prohibited. The school district will completely and periodically delete information from the system.

Emails sent within the district's domain are secure in that the content remains encrypted from sender to receiver. Alternatively, email sent outside of the tewksbury.k12.ma.us domain leaves the encrypted Google workspace domain and travels across the open internet unencrypted. Users should not send confidential student information via email to outside parties.

Legal Implications of Electronic Mail (Email)

For the purpose of this procedure, email is defined as messages created and received on an electronic mail system. The email message may be text or word processing documents, spreadsheets or other data compilations transmitted through such a system. Email created or received by an employee of a government unit is a public record. In Massachusetts, the term "public record" is broadly defined to include all documentary materials or data created or received by any officer or employee of any governmental unit, regardless of physical form or characteristics. G.L. c. 4, sec. 7(26). Email is therefore a public record and subject to the requirements of the Public Records Law G. L. C. 66. Email messages are subject to public access through the Public Records Law G. L. C. 66. Sec.10. A determination as to whether an email message is exempt from disclosure depends upon the content of the message. G. L.C. 4. Sec. 7(26)(a- m).

Email messages may be sought through the discovery process in litigation and may be admissible in evidence. Like all electronically created and stored records, email is subject to the rules of evidence

and a judge will rule on its admissibility. Refer to the Commonwealth of Massachusetts Public Records Division SPR- Bulletin No. 1-99 dated February 16, 1999 for additional information.

Network Use Limitations

TPS's computer networks may not be used to disseminate commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, self- replicating programs, etc.), or any other unauthorized materials. Staff and students may not use the school system's Internet connection to download games or other entertainment software or to play non-educational games over the Internet. Additionally, you may not use the computer network to display, store or send (by email or any other form of electronic communication such as bulletin boards, chat rooms, Usenet groups, etc.) material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, unlawful, defamatory or otherwise inappropriate.

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources. As such, the user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include but are not limited to, streaming music or videos for non- educational purposes, sending chain letters, spending, playing online games, or otherwise creating unnecessary loads on network traffic associated with nonbusiness-related uses of the Internet.

Wireless "Guest" network access is provided for non-Tewksbury School district devices throughout district buildings. All non-district devices must only connect to the "Guest" network. Access to the network(s) is monitored, any violations of the above mentioned statutes can result in the offending device from being excluded from the network(s).

Social/Web 2.0 / Collaborative Content

Recognizing the benefits that collaboration brings to education, TPS may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among TPS users and the global user community. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored and restricted. Users should be careful not to share personally- identifying information online. Social media accounts created for school use are considered public record. See Legal Implications of Electronic Mail (Email) above. All users should adhere to the Social media policy IJNDD.

Mobile Devices

TPS may provide users with mobile computers (Classroom carts or 1:1 Program) or other devices to promote learning outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network. Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should immediately report any loss, damage, or malfunction to IT staff.

Users may be financially accountable for any damage resulting from negligence or misuse. Use of school issued mobile devices off the school network may be monitored. Devices are to be returned to TPS in working order upon leaving the district or when requested by TPS.

Personally-Owned Devices

All devices are considered use at your own risk. The School District is not accountable for loss, damage, theft, etc.

Please remember, this Acceptable Use Procedure applies to privately-owned devices accessing the TPS network, the TPS Internet connection, and private networks/Internet connections while on school property. Virus protection for PC's is required.

Users who cannot access the TPS network or who may have technical issues with their technology tool need to take care of this issue by working with the user's manual that came with the device outside of the classroom. These are not TPS devices and TPS will not allocate resources to troubleshoot issues.

Users have the option to join TPS District's "Guest" network with a personally-owned mobile device. While using the Guest network users are to abide by The School District's Acceptable Use Policy. The district reserves the right to ban any user device from the network.

Students should keep personally-owned devices (including but not limited to laptops, tablets, cell phones, network attached devices, wireless hotspots) turned off and put away during school hours. Because of security concerns, when personally-owned mobile devices are used on campus, they must be used over the school network.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. Reasonable safeguards include but are not limited to setting and maintaining passwords, locking and security unattended technology devices. This applies to all TPS and personally owned devices. Do not open or distribute files or programs of unknown or untrusted origin. If you believe a computer or mobile device you are using might be infected with a virus, do not attempt to remove the virus yourself or attempt to download any programs to help remove the virus. Please shut the device down and alert TPS IT Services.

TPS IT Services has installed antivirus on district computers. It is prohibited to attempt to disable or remove such software. Periodic computer reboots are required so computer anti-virus software functions properly. This is the responsibility of the user of the device.

Devices with the intention of hacking, collecting, monitoring, generating, manipulating, or intercepting data, or any intent deemed malicious or unacceptable by TPS are not permitted for use in the TPS District.

You are responsible for any misuse of your account (network, email, or otherwise), even if the inappropriate activity was committed by another person. Therefore, you must take steps to ensure that others do not gain unauthorized access to your account. In addition, you may not use your account to breach the security of another account or attempt to gain unauthorized access to another network or server.

Your password provides access to your account. Sharing your password and account access with unauthorized users is prohibited. You should take care to prevent others from using your account by keeping your password secure since you will be held responsible for such use. Do not leave an unsupervised computer logged on to the network, lock all devices when not in use.

Application Downloads/Installations

The TPS district computing devices have been configured by the IT Services Staff. TPS users should not download, attempt to download, run or install any programs onto school computing devices without express permission from the IT Services Director. Only software purchased by TPS should be installed on TPS computing devices, free, pirated, or self purchased software should not be installed on TPS computing devices.

Digital Resources

In order to protect student data privacy in compliance with COPPA, FERPA , PPRA, and HIPPA, all Digital resources must have a signed Data Privacy Agreement (DPA) on file. Any resource without a signed DPA will require parent/guardian approval for use. In the case that there is no signed DPA and the parent/guardian does not grant permission, the resource is not permitted to be utilized in TPS.

Net Etiquette

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner. Users should recognize that among the valuable content online there is also unverified, incorrect, or inappropriate content. Users should only use trusted sources when conducting research via the Internet. Users should remember not to post anything online that they wouldn't want students, parents, teachers, or future colleges or employers to see. Once something is online, it's out there—and can sometimes be shared and spread in ways you never intended.

Plagiarism

Users should not plagiarize (or use as their own without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

Users should never share theirs or anyone else's personal information, including phone number, address, social security number, birthday, or financial information, over the Internet or other means

of communications without adult permission. Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet in real life someone they meet online without parental permission. If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

TPS makes an attempt to protect private information but users who submit personal information online do so at their own risk.

Cyber-bullying

Cyber-bullying will not be tolerated. Harassing, denigrating, impersonating, outing, tricking, excluding, and cyber-stalking are all examples of cyber-bullying. Don't be mean. Don't send emails or post comments or pictures with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyber-bullying can be a crime. Remember that your activities are monitored and retained.
Cyber-bullying is covered under both Massachusetts state law Chapter 71 sec. 37o and TPS Bullying Prevention Policy **JICFB**

Virtual Meetings

The Tewksbury Public School community expects that all students will be good digital citizens who practice safe, and legal use of technology in a positive way.

It is expected that everyone in each household engaged in a session will respect student confidentiality at all times. As such, no other individual other than the student or guardian should be present during live sessions. It is recommended that participants should present themselves in a space that is as private as possible, and/or with their backs to a solid surface.

In order to ensure that every student in the class can participate and/or view a live virtual session, whole class sessions may be recorded by the teacher so that it can be accessed at a later time. Or, teachers may record their presentation in advance to provide it to students who cannot attend a live session. Recording of any portion of any session by any party other than the teacher running the session is not permitted. This includes posting excerpts of, or about a session on any form of social media.

TPS staff reserves the right to end any student's participation in a live session if their presence, that of a parent/guardian, or any third party or activity, causes a disruption of the educational process during the distance learning session. If live session rights are terminated, TPS can determine alternative means to provide the learning opportunity.

Vandalism/Tampering

Any verified acts of vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy the data of another user, the TPS network, computing devices, or other networks that are connected to our system through the Internet. This includes, but is not limited to, the uploading or creation of computer viruses, physical damage, and rogue devices on the network or otherwise. Any tampering with a device including but not limited to the removal of admin user accounts, the removal of the red tag or any other identifying information on the device would also violate this policy (IJNDB-R).

Privacy

Staff and students are given access to computers and the Internet to assist them in furthering the educational process. Users should have no expectation of privacy in anything they create, store, send or receive using TPS's computer equipment and or accounts. In addition TPS, through its designees, reserves the right to monitor, examine, evaluate and disclose all aspects of the technology resources and their use.

Tewksbury Public Schools is committed to protecting private information of staff and students contained within emails or other online transmissions.

While we cannot guarantee the privacy or confidentiality of information within electronic documents, which is public information, the following procedure will help to protect the privacy and confidentiality of such information.

1. Remember when sending emails regarding students to use ONLY the first initial of both their first and last name eg: John Smith would be J.S.
2. Remember when sending emails regarding staff to use ONLY the staff member's initials and job eg: John Smith teacher would be J.S. teacher.
3. TPS is a member of the Student Data Privacy Consortium (SDPC) which helps us to vet all of our online resources to protect student data.
4. Digital resources that collect student data are not allowed for use by TPS staff and students unless there is a signed DPA or specific parent permission has been obtained.

The District monitors and filters all network traffic localAll network traffic, local or otherwise or related to District owned devices and/or accounts are subject to filtering and monitoring under this AUP. The purpose of monitoring data is for student and staff safety. TPS filters and monitors all traffic when you are on campus utilizing the schools Wireless or wired network on any device (personal or school owned) and traffic when utilizing a district account or district devices on or off campus. All student generated content is monitored for student safety. If

Determine content filtering / surveillance policy. This will clearly document the level and purpose of surveillance of student generated content. If student generated content will continue to be monitored /surveilled then parents and students need to be clearly informed of this practice.

Leaving the District

Upon leaving the district, a user may obtain a copy of documents created using school accounts per approval of the building principal/administrator. The user should reach out to the building principal/administrator prior to their last day to obtain approval. The building principal should then contact IT for the procedure. All accounts will be deactivated upon leaving the district. Devices and security cards badges are to be returned to TPS in working order upon leaving the district.

Limitation of Liability

TPS will not be responsible for damage or harm to persons, files, data, or hardware.

While TPS employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. TPS will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Examples of Acceptable Use

I will:

- Use Technology for School Related activities
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat school resources carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative Technologies.
- Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits.
- Cite sources when using online sites and resources for research.
- Recognize that use of school technologies is a privilege and treat it as such.
- Be cautious to protect the safety of myself and others.
- Help to protect the security of school resources.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies

Examples of Unacceptable Use

I will not:

- Share student information in accordance with FERPA. (All Digital resources that collect student information need to have a signed DPA by the district or parent permission for use.)
- Use school technologies in a way that could be personally or physically harmful.
- Attempt to find inappropriate images or content; intent to seek inappropriate images or

content is a violation of this Acceptable Use Procedure.

- Create a personal mobile “hot-spot” or use a “proxy site” for the purpose of circumventing network safety measures and filtering tools.
- Create, distribute or deploy multi-user servers or gaming software on or within the TPS network.
- Use proxy avoidance software, tools, and websites.
- Use remote management software, tools, and websites.
- Use VPN software, tools, and websites.
- Engage in cyber-bullying, harassment, or disrespectful conduct toward others.
- Use obscene, inflammatory, harassing, threatening, or abusive language or images
- Try to find ways to circumvent the school’s safety measures and filtering tools; intent to circumvent safety measures and filtering tools is a violation of this Acceptable Use Procedure.
- Use school technologies to send spam or chain mail.
- Plagiarize content I find online.
- Post or otherwise disclose personally-identifying information, about myself or others.
- Agree to meet someone I meet online in real life.
- Use language online that would be unacceptable in the classroom.
- Use school technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, or content that isn’t intended for my use.
- Access materials or use email for nonacademic purposes or for purposes that are not approved by the staff member in charge
- Tamper with data and files being used by others.
- Use school accounts for personal messages, political lobbying, union messages, gambling, or business transactions, advertising, or commercial (offering or providing products or services) activities.
- Use or transmit materials that violates copyright laws

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Violations of Acceptable Use Policy (IJNDB-R)
Violations of this policy may have disciplinary repercussions,
including:

- Suspension or termination of network, technology, or computer privileges;
- Notification to parents;
- Detention or suspension from school and school-related activities;
- Employment disciplinary action, up to and including termination of employment;
- Legal action and/or prosecution.

The Tewksbury Public Schools will provide staff with Internet guidelines and training and support in

the appropriate and effective use of the internet. The school system will inform parents about Internet guidelines through the use of letters, school newsletters, and handbooks. Additionally, the Tewksbury Public Schools will continually evaluate tools and software which can potentially assist staff in implementing guidelines, effectiveness, manageability, and any cost for initial purchase and upgrades will be considered.

TEWKSBURY PUBLIC SCHOOLS
STATEMENT OF RESPONSIBILITIES

Staff, students and parents are to read the *Tewksbury Public Schools Technology Acceptable Use Procedures (Pertaining to IJNDB – Acceptable Use Policy – Technology - click here to access procedures and policy)*. These documents can also be found on the TPS District Webpage: http://www.tewksbury.k12.ma.us/

User Expectations

I have read, understand and will follow the Tewksbury Acceptable Use Procedure, pertaining to the *IJNDB – Acceptable Use Policy – Technology - click here to access procedures and policy).* My commitment to responsible digital citizenship is a critical component in mastering 21st century skills. If I break this agreement, the consequences could include suspension of computer privileges and/or disciplinary action. I also understand the school network and email accounts are owned by Tewksbury Public School and that Tewksbury Public Schools has the right to access any of the information used through the mediums provided through the school at any time. I understand that technology is provided for educational purposes in keeping with the academic goals of Tewksbury Public Schools, and that use for any other purpose is inappropriate. I recognize it is impossible for the school to restrict access to all controversial materials, and I will not hold the school responsible for materials acquired on the school network. I understand that computer activities at home should be supervised as they can affect the academic environment at school.

Parents/Guardians should read this Acceptable Use Procedure. Parents/guardians should discuss the technology use responsibilities with their children. Questions and concerns can be forwarded to the Tewksbury Public Schools and appropriate offices.

Parents/guardians and Staff agree to accept financial responsibility for any expenses or damages incurred as a result of their or their student's inappropriate or illegal activities on the Tewksbury Public Schools network. Parents/Guardians and staff agree to reimburse Tewksbury Public Schools for any expenses or damages incurred in the use of district owned technology devices.

By signing this document below, I acknowledge that I have read and understand the Tewksbury Public Schools Technology Acceptable Use Procedures (Pertaining to IJNDB – Acceptable Use Policy – Technology) and know I can contact my school principal if I have further questions.

_____	_____
User Name (please print)	Parent/Guardian if under 18 years old (please print)
_____	_____
User Signature	Parent/Guardian Signature
_____	_____
Date	Date

File: IJNDB

ACCEPTABLE USE POLICY - TECHNOLOGY

Purpose

The Tewksbury Public Schools shall provide access for employees and students to the system/network, including access to external networks, for limited educational purposes. Educational purposes shall be defined as classroom activities, career and professional development, and high quality self-discovery activities of an educational nature. The purpose of the system/network is to assist in preparing students for success in life and work by providing access to a wide range of information and the ability to communicate with others. The system/network will be used to increase communication (staff, parent, and student), enhance productivity, and assist staff in upgrading existing skills and acquiring new skills through a broader exchange of information. The system/network will also be utilized to provide information to the community, including parents, governmental agencies, and businesses.

Availability

The Superintendent or designee shall implement, monitor, and evaluate the District's system/network for instructional and administrative purposes.

Access to the system/network, including external networks, shall be made available to employees and students for instructional and administrative purposes and in accordance with administrative regulations and procedures.

Access to the system/network is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations and procedures governing use of the system and shall agree in writing to comply with such regulations and procedures. Noncompliance with applicable regulations and procedures may result in suspension or termination of user privileges and other disciplinary actions consistent with the policies of the Tewksbury Public Schools. Violations of law may result in criminal prosecution as well as disciplinary action by the Tewksbury Public Schools.

Acceptable Use

The Superintendent or designee shall develop and implement administrative regulations, procedures, and user agreements, consistent with the purposes and mission of the Tewksbury Public Schools as well as with law and policy governing copyright.

Monitored Use

Electronic mail transmissions and other use of electronic resources by students and employees shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use for instructional and administrative purposes.

Liability

The Tewksbury Public Schools shall not be liable for users' inappropriate use of electronic resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users.

The Tewksbury Public Schools shall not be responsible for ensuring the accuracy or usability of any information found on external networks.

SOURCE: MASC Adopted: April 14, 2015 Policy Link

File: IJNDB-R - ACCEPTABLE USE POLICY - TECHNOLOGY
Administrative Procedures for Implementation

1. Commercial use of the system/network is prohibited.
2. The district will provide training to users in the proper use of the system/network.
3. The district will provide each user with copies of the Acceptable Use Policy and Procedures.
4. Copyrighted software or data shall not be placed on the district system/network without permission from the holder of the copyright and the system administrator.
5. Access will be granted to employees with a signed access agreement and permission of their supervisor.
6. Access will be granted to students with a signed access agreement and permission of the building administrator or designee(s).
7. Account names will be recorded on access agreements and kept on file at the building level.
8. Initial passwords provided by the network administrator should be set to expire on login.
9. Passwords shall expire at the end of each school year.
10. Passwords are confidential. All passwords shall be protected by the user and not shared or displayed.
11. Principals or their designee will be responsible for disseminating and enforcing policies and procedures in the building(s) under their control.
12. Principals or their designee will ensure that all users complete and sign an agreement to abide by policies and procedures regarding use of the system/network. All such agreements are to maintained at the building level.
13. Principals or their designee will ensure that training is provided to users on appropriate use of electronic resources.
14. Principals or their designee shall be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure proper use of electronic resources.
15. Principals or their designee shall be responsible for establishing appropriate retention and backup schedules.
16. Principals or their designee shall be responsible for establishing disk usage limitations, if needed.
17. Individual users shall, at all times, be responsible for the proper use of accounts issued in their name.
18. The system/network may not be used for illegal purposes, in support of illegal activities, or for any activity prohibited by district policy.
19. System users shall not use another user's account.
20. System users should purge electronic information according to district retention guidelines.
21. System users may redistribute copyrighted material only with the written permission of the copyright holder or designee. Such permission must be specified in the document or in accordance with applicable copyright laws, district policy, and administrative procedures.
22. System administrators may upload/download public domain programs to the system/network. System administrators are responsible for determining if a program is in the public domain.
23. Any malicious attempt to harm or destroy equipment, materials, data, or programs is prohibited.
24. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of district policy and/or as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creation of computer viruses.
25. Vandalism will result in the cancellation of system privileges and will require restitution for costs associated with hardware, software, and system restoration.
26. Forgery or attempted forgery is prohibited.
27. Attempts to read, delete, copy, or modify the electronic mail of other users or to with the ability of other users to send/receive electronic mail is prohibited.
28. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and other inflammatory language is prohibited.

29. Pretending to be someone else when sending/receiving message is prohibited.
30. Transmitting or viewing obscene material is prohibited.
31. Revealing personal information (addresses, phone numbers, etc.) is prohibited.
32. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's system/network.
33. Internet users will be held responsible for the appropriate use of the school district's electronic resources.
All communications, sent or received, on a publicly owned resource may be subject to public record laws.
A user who violates district policy or administrative procedures will be subject to suspension or termination of system/network privileges and will be subject to appropriate disciplinary action and/or prosecution.

SOURCE: MASC Policy REVISED: April 14, 2015 Policy Link