GT

STAFF TECHNOLOGY USE POLICY AND AGREEMENT

Introduction

This Policy and Agreement outlines the acceptable use of technology hardware, software, systems, networks, websites, Internet connections and /or other equipment, hereafter referred to as "technology," belonging to, or in possession and/or control of, the Wrentham Public Schools (WPS). This Policy shall apply to all WPS employees, officers, volunteers, agents or other representatives hereinafter referred to as "Users," who utilize WPS technology. All users are required to sign this Agreement confirming that he/she read and understands this Policy and agrees to abide by this Policy.

Additionally, this Policy and Agreement shall be accessible at all times on the WPS website and in the offices of every building principal and the superintendent. All Users are required, and hereby agree, to remain up-to-date in their knowledge of the Policy and to comply with the Policy as updated at all times.

The superintendent, as liaison to the school committee, will inform staff, on a timely basis, of any and all changes made to this policy.

Any failure to comply with this Policy may constitute misconduct by the User and may result in discipline and/or legal action against the User.

I. Protection Measures

A. At the beginning of each school year, the superintendent or designee will discuss with staff members the contents of the Staff Technology Use and Policy Agreement.

B. At the beginning of each school year, the classroom teacher will read and discuss with students the contents of the Student Guidelines for Yearly Review document.

C. Through the use of network security, firewalls, antivirus, anti-spam and content filtering, the WPS will place the highest priority on its attempt to protect all users and all data.

D. Students will not be given access to e-mail, texting, newsgroups or chatting.

E. Only the first name and the first initial of the last name of a student will be used on the WPS website. The name of a student will not be associated with his/her picture.

F. Students may create web pages. All material placed on that webpage must be pre-approved by a WPS teacher.

G. The WPS filtering system attempts to block user access to inappropriate and/or harmful text on the Internet. The filter setting is kept at the most restrictive level. Because the Internet is complex and ever-changing, the filtering system can never be 100% reliable. In the event that the filtering software is unsuccessful and children gain access to inappropriate and/or harmful material, the WPS will not be liable.

The following guidelines should be followed:

1. Students will have teacher-supervised access to the Internet. Monitoring student use at every moment is not a reasonable expectation. Even with all the protection

measures in place, it is possible for a student to accidentally or purposely find material that is not consistent with the WPS educational mission.

2. If a student mistakenly accesses inappropriate information, he/she should immediately close the connection to the site and refrain from downloading any material. The student should then report the incident to the classroom teacher. The teacher will then report the incident to his/her building principal and provide the address of the site to the Director of Technology.
3. Each student is expected to take individual responsibility for his/her appropriate use of the Internet.
4. Best practice is to provide students with previewed websites that address the topic and meet the educational mission of the WPS. If students do need to search on the Internet, they should be using student safe search engines that are provided on the WPS website. Staff should be aware that searching for clip art or images is particularly vulnerable to unfiltered inappropriate content.

H. Online communication is critical to our students' learning of 21st Century Skills. Web 2.0 tools such as blogs, wikis, podcasts, etc. offer a vehicle for student expression. The primary responsibility to students is their safety. The following guidelines should be followed:

1. If teachers are trained with Web 2.0 tools then they will supervise any classroom use of Web 2.0 tools.
2. Access to the Web 2.0 tools interactivity should require a username and password and be limited to staff and students within the WPS. Individuals outside the school system will have viewing access only.
3. Students will only share their username and password with their teachers and their parents.
4. Students using Web 2.0 tools are expected to act safely by keeping all personal information out of their posts. This includes, but is not limited to, last names, address, phone numbers and photographs.

I. The WPS will maintain compliance with the Children's Internet Protection Act (CIPA) at all times.

II. Privacy

A. No user shall have any expectation of privacy regarding his/her use of technology. The WPS can and does monitor all computer use. All Internet usage, messages, data, and information viewed, created, sent or retrieved through WPS technology are the property of the WPS. The WPS reserves the right to monitor, inspect, copy, review, delete, destroy, maintain and/or store all Internet usage, messages, data, and information. As public material, all information maintained on WPS technology is subject to the Massachusetts Public Records law. This information may be disclosed to law enforcement or other third parties without prior notice to or consent of the user, sender or receiver.

B. Deleting an e-mail only deletes it from the user's computer and/or mailbox. Any e-mail communication sent through the WPS technology will be kept separate from the user's computer, and is the property of the WPS. These e-mails will be kept for a period of seven years.

III. Personal Responsibility

A. By signing this Policy and Agreement, the user agrees to follow all rules outlined in the Policy. WPS provides users with access to WPS technology to help them perform their job

responsibilities. Each user shall be personally responsible for his/her use of WPS technology, and shall use WPS technology only in conformance with this Policy.

B. In this age of "social networking" school employees must keep in mind that they are at all times role models, and this extends even to non-work times during which they are using their personal computers. Communications on social networking sites and "blogs" are typically public in nature, and school employees must be conscious of the need to behave as role models in all of their public communications.

C. WPS may, acting in its sole discretion, limit or deny the privilege of access to WPS technology to any user at any time.

IV. Acceptable Uses

A. WPS provides access to its computer networks and the Internet primarily for educational and administrative purposes. Approved uses include, but are not limited to, research, communication and activities that support WPS' educational mission.

B. Before and after school hours, or at other times as permitted by the WPS, users may utilize WPS technology for non-school business, including research, browsing, or for the sending and receiving of non-school business e-mails. Non-school e-mails sent and received through the WPS network are also kept for a period of seven years.

V. User Responsibilities

Users of WPS technology are expected to abide by accepted uses. These include, but are not limited to, the following:

A. Users should abide by generally accepted rules of Internet network etiquette including common courtesy, politeness, and respect.

B. Users will abide by the Bullying and Cyber Bullying Policy.

C. Passwords are confidential and should not be shared or displayed. Passwords may not be changed without permission of the Director of Technology.

D. E-mails should be deleted on a regular basis to conserve space and to help optimize the speed and efficiency of the e-mail system.

E. Backing up or transferring of locally stored files will be the sole responsibility of the user. The technology staff will routinely re-image or re-format the computer's hard drive without checking for locally stored files. The technology staff will not attempt to recover any locally stored files due to hardware failure.

F. Voicemail and e-mail should not be used for time sensitive messages from parents. WPS staff should encourage and remind parents that time sensitive messages must be handled by the respective offices.

G. Due to storage space limitations, personal pictures and videos may not be stored on WPS technology.

H. E-mail attachments are often a source of viruses or spyware. Staff members should never open attachments from an unknown user.

I. E-mails should be opened discreetly due to the unknown content contained. Visual and auditory distance from students should be maintained.

J. E-mails sent to groups of parents should be sent using Bcc. This protects the privacy of each parent's e-mail address.

K. Technology issues regarding security, misuse and damage should be immediately reported to the technology staff.

L. Software loaded onto computers must adhere to all copyright laws and be loaded by a technology staff member. Personally purchased software must be "donated" to the school for the time period that it resides on WPS technology with the proof of license or media stored at the WPS.

M. Because of the very restrictive setting of the filtering software, educationally appropriate websites could be blocked. A staff member can request that the site be unfiltered only after previewing the site and deeming it appropriate for student viewing. A request to unblock the site can then be sent to the technology help desk.

N. Video conferencing is used for educational purposes only.

VI. Unacceptable Uses of Technology

Users of WPS technology are prohibited from unacceptable uses. These include, but are not limited to, the following:

A. Using the Internet in a manner that would violate any federal, state, or local statute, regulation, rule or policy.

B. Using threatening, defamatory, discriminatory, or harassing language or language that constitutes a criminal offense or that is detrimental to or in opposition to the WPS' educational mission in any e-mail message or other Internet communication.

C. Displaying or downloading any kind of sexually explicit offensive image or document. In addition, sexually offensive material may not be archived, stored, distributed, edited, or recorded using WPS technology.

D. Knowingly engaging in any activity that could result in damage to WPS technology.

E. Sharing passwords or assigned accounts, without the express authorization of the WPS.

F. Engaging in activities designed to or that may potentially expose WPS technology or other computers to computer viruses, other harmful software, attempts to access technology function in unauthorized ways, or other injury or damage.

G. E-mailing students who are unrelated to the user for non-school business-related reasons.

H. School business use of instant messaging, chat room, or social networking (facebook, my space, etc.) for communication with students is prohibited.

I. Unauthorized copying, downloading, or distributing of copyrighted or pirated software, materials or data. This includes, but is not limited to: e-mail, text files, program files, image files, database files, sound files, music files, and video files.

J. Providing private and/or confidential information about any individual other than the user, or the user's immediate family, over WPS technology.

K. Using WPS technology to transmit or display material confidential to the WPS to uninvolved parties without the authorization of the WPS. This includes material posted in chat rooms, newsgroups, blogs, or other public forums.

L. Downloading entertainment software or games, except where the user obtains the prior written authorization of the WPS.

M. Installing and/or operating peer-to-peer software.

N. Attempting to harm, maliciously modify, or destroy data that has been created by another.

O. Plagiarizing.

P. Spamming or the unauthorized use of WPS distribution lists for e-mails. This includes creating or forwarding chain letters or pyramid schemes of any type.

VII. Failure to Follow Policy

Violating any of the guidelines listed above can, at the discretion of the WPS, result in:

A. Restricted technology access.

B. Loss of technology access.

C. Disciplinary action against the user that might include termination of employment.

D. Referral to law enforcement personnel and/or legal action including, but not limited to, criminal or civil prosecution and/or penalty under appropriate state and federal laws.

VIII. Warranties/Indemnifications

The WPS makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its technology provided under this policy. The WPS shall not be responsible for any claims, losses, damages, injuries or costs or fees (including attorney's fees) of any kind suffered or incurred, directly or indirectly, by any user arising from use of the WPS' technology

By signing this policy and agreement, the user takes full responsibility and agrees to hold harmless and indemnify the WPS, its Internet Service Provider (ISP), the town of Wrentham, and all of the WPS', its ISP's officers, and the town's employees, agents, servants, representatives, administrators, teachers, volunteers and staff from any and all claims, losses, damages, injuries or costs or fees (including attorneys fees) of any kind resulting from the user's access to the WPS' technology, including, but not limited to, any fees or charges incurred through purchased of goods or services by the user.

IX. Liability

The WPS shall not be liable for any users' inappropriate use of electronic resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users. The WPS shall not be responsible for ensuring the accuracy, safety, harmlessness, or usability of any information found on the Internet. The WPS shall not be responsible for any claims, losses, damages, injuries, or costs or fees (including attorney's fees) of any kind suffered or incurred, directly or indirectly, by any user arising from use of the WPS' technology.

I hereby state that I have read and understood and agree to abide by the terms of this policy.

_____

User Name (please print)

_____

User Signature

_____

Date

Adopted March 22, 2011
Revised October 26, 2014