WEYMOUTH Public Schools

Strong Schools Strong Community

2023

Guidelines for Implementation of Acceptable Use Policy for Digital Information, Communication, and Technology Resources

ACCEPTABLE USE POLICY AND GUIDELINES

Scope of Policy

Weymouth Public Schools (WPS) provides access to technology devices, Internet, and data systems to employees and students for educational and business purposes. This Acceptable Use Policy (AUP) governs all electronic activity of employees using and accessing the district's technology, Internet, and data systems regardless of the user's physical location.

Guiding Principles:

- Online tools, including social media, should be used in our classrooms, schools, and offices to increase community engagement, staff and student learning, and core operational efficiency.
- WPS has a legal and moral obligation to protect the personal data of our students, Legal Guardians, and staff.
- WPS should provide a baseline set of policies and structures to allow schools to implement technology in ways that meet the needs of their students.
- All students, Legal Guardians, and staff must know their rights and responsibilities outlined in the Acceptable Use Policy and government regulations.
- Nothing in this policy shall be read to limit an individual's constitutional rights to freedom of speech or expression or to restrict an employee's ability to engage in concerted, protected activity with fellow employees regarding the terms and conditions of their employment.

Compliance Requirement for Employees

The Acceptable Use Policy is reviewed annually by the Superintendent and Director of Educational Technology. Technology users are required to verify that they have read and will abide by the Acceptable Use Policy annually.

Student AUP & Contract

Copies of the Acceptable Use Policy and the student contract for Internet use are included in the Guide to WPS for Legal Guardians & Students, given to all students at the beginning of the school year. The Student Contract for Internet Use must be completed and signed by all students and their parent/guardian after going over the AUP together. The signed contract must be returned to the school before the student may begin using the Internet.

Consequences of Breach of Policy
Use of all WPS technology resources is a privilege, not a right. By using WPS Internet Systems and devices, the user agrees to follow all WPS regulations, policies and guidelines. Students and staff are encouraged to report misuse or breach of protocols to appropriate personnel, including building administrators, direct supervisors and to the WPS Educational Technology Department (WPS EDTECH). Abuse of these privileges may result in one or more of the following consequences:

- Suspension or cancellation of use or access privileges.
- Payments for damages or repairs.
- Discipline under appropriate School Department policies, up to and including termination of employment, subject to any collective bargaining obligations.
- Liability under applicable civil or criminal laws.

Definitions

Freedom of Information Act (FOIA) - The FOIA is a law that allows for the release of government documents at the request of an individual. A FOIA request can be made to the WPS for electronic documents/communications stored or transmitted through district systems unless that information could be detrimental to governmental or personal interests. For more information, visit http://www.foia.gov/

Family Educational Rights and Privacy Act (FERPA) - The FERPA law protects the privacy, accuracy, and release of information for students and Legal Guardians of WPS. Personal information stored or transmitted by agents of WPS must abide by FERPA laws and the WPS is required to protect the integrity and security of student and family information. For more information, visit http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

with local, state, and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies or government regulations.
Guidelines for Online Communication

1. Communication with students should not include content of a personal nature.
2. When communicating with parents/guardians of students, employees should use email addresses and phone numbers listed in the Student Information System (SIS) unless steps have been taken to verify that the communication is occurring with a parent/guardian that has educational rights for the student.
3. When communicating with a parent/guardian, refrain from discussing any non-related students when possible.
4. Employees who use internal or external social media (blogs, Twitter, etc.) are expected to refrain from discussing confidential information and/or discussing specific students. Information that can be traced back to a specific student or could allow a student to be publicly identified should not be posted on any social media sites.
5. When using social media, employees are expected to refrain from posting any negative comments online about students.
6. Employees are required to notify their principal before setting up an online site

to facilitate student learning. Employees are encouraged to monitor/moderate online communication to the best of their abilities.

7. Employees should not add any students/former students or parents as 'friends' or contacts on
8. Social media unless the site supports classroom instruction or school business.
9. Employees may communicate with WPS graduates (+18 years old) on social media but should be advised to maintain professionalism and caution when communicating online.
10. Employees who add parents/guardians of students as 'friends' or contacts on social media must
11. Maintain professionalism to avoid any appearance of conflict of interest.
12. Avoid responding to spam or phishing attempts that require a user to click on any links or to provide any account information. Note: WPS will never ask for a user's account password for any purpose and users are advised to report any suspicious requests for account information directly to the WPS Educational Technology Department.

Solicitation

Web announcements and online communication promoting a business are prohibited by the WPS Solicitation Policy. The Superintendent's Office may make exceptions if benefits are judged sufficient to merit exception.

Use of Copyrighted Materials

Violations of copyright law that occur while using the WPS network or other resources are prohibited and have the potential to create liability for the district as well as for the individual. WPS staff and students must comply with regulations on copyright plagiarism that govern the use of material accessed through the WPS network.

Users will refrain from using materials obtained online without requesting permission from the owner if the use of the material has the potential of being considered copyright infringement. WPS will cooperate with copyright protection agencies investigating copyright infringement by users of the computer systems and network of the WPS.

Network Usage:

Network access and bandwidth is provided to schools for academic and operational services. WPS reserves the right to prioritize network bandwidth and limit certain network activities that are negatively impacting academic and operational services. Users are prohibited from using the WPS network to access content that is inappropriate or illegal, including but not limited to content that is pornographic, obscene, illegal, or promotes violence.

Network Filtering & Monitoring:

As required in the Children's Internet Protection Act (CIPA), WPS is required to protect students from online threats, block access to inappropriate content, and monitor Internet use by

minors on school networks. WPS EDTECH is responsible for managing the district's Internet filter and will work with the WPS community to ensure the filter meets the academic and operational needs of the district while protecting minors from inappropriate content.

By authorizing use of technology resources, WPS does not relinquish control over materials on the systems or contained in files on the systems. There is no expectation of privacy related to information stored or transmitted over the WPS network or in WPS systems. WPS reserves the right to access, review, copy, store, or delete any files (unless other restrictions apply) stored on WPS computers and all employee and students communication using the WPS network. Electronic messages and files stored on WPS computers or transmitted using WPS systems may be treated like any other school property. District administrators and network personnel may review files and messages to maintain system integrity and, if necessary, to ensure that users are acting responsibly. WPS may choose to deploy location tracking software on devices for the sole purpose of locating devices identified as lost or stolen.

Personal Use:

WPS recognizes that users may use WPS email, devices, and network bandwidth for limited personal use; however, personal use should not interfere with or impede district business and/or cause additional financial burden on the district. Excessive use or abuse of these privileges can be deemed in violation of the Acceptable Use Policy.

Network Security:

The WPS Wide Area Network (WAN) infrastructure, as well as the building-based Local Area Networks (LANs) are implemented with performance planning and appropriate security measures in mind. Modifications to an individual building network infrastructure and/or use will affect LAN performance and will reduce the efficiency of the WAN. For this reason, any additional network electronics including, but not limited to, switches, routers, and wireless access points must be approved, purchased, installed, and configured solely by WPS EDTECH to ensure the safety and efficiency of the network. Users are prohibited from altering or bypassing security measures on electronic devices, network equipment, and other software/online security measures without the written consent of the Director of Educational Technology.

Data & Systems:

Access to view, edit, or share personal data on students and employees maintained by WPS central offices, individual schools, or by persons acting for the district must abide by local, state, and federal regulations, including the Family Educational Rights and Privacy Act. Student and staff information and data may only be shared with individuals deemed eligible to have access by the person(s) responsible for oversight of that data. Outside parties and/or non-WPS individuals requesting protected data must receive approval from the Office of the Legal Advisor and have a non-disclosure agreement with the WPS. Data stored on WPS systems including but not limited to: computers, network drives, Google drives, etc. are property of WPS. Individuals requesting ongoing access to data through WPS systems are required to have a designated WPS administrator who will act as a "sponsor" to ensure the safety of the data.

Electronic Transmission of Data:

When educational records or private data are transmitted or shared electronically, staff are expected to protect the privacy of the data by password-protecting the record/file and only using WPS systems to transmit data. Staff are also expected to ensure records are sent only to individuals with a right to said records and must take reasonable measures to ensure that only the intended recipients are able to access the data.

Passwords:

Users are required to adhere to password requirements set forth by the WPS when logging into school computers, networks, and online systems. Users are not authorized to share their password and must use extra caution to avoid email scams that request passwords or other personal information.

Media & Storage:

All local media (USB devices, hard drives, CDs, flash drives, etc.) with sensitive data must be securely protected with a password and/or encrypted to ensure the safety of the data contained. Use of cloud-storage services for storage or transmission of files containing sensitive information must be approved by the Office of the Legal Advisor and WPS. Users are encouraged to use WPS approved data/information systems for the storage and transmission of sensitive data whenever possible and avoid storage on local hardware that cannot be secured.

Electronic Devices:

WPS defines electronic devices as, but not limited to, the following:

a. Laptop and desktop computers, including like-devices
b. Tablets
c. Wireless email and text-messaging devices, i.e., iPod
d. Smartphones
e. Donated devices

Device Support:

WPS provides basic installation, synchronization, and software support for WPS-issued electronic devices. Devices must be connected to the WPS network on a regular basis to receive software and antivirus updates and for inventory purposes. Password protection is required on all WPS-issued electronic devices to prevent unauthorized use in the event of loss or theft. Users are responsible for making periodic backups of data files stored locally on their devices.

Loss/Theft:

Users must take reasonable measures to prevent a device from being lost or stolen. In the event an electronic device is lost or stolen, the user is required to immediately notify appropriate school staff and/or their direct supervisor, local authorities, and the WPS Educational Technology Department. The WPS will take all reasonable measures to recover the lost property and to ensure the security of any information contained on the device.

Return of Electronic Devices:

All technology purchased or donated to the WPS is considered district property and any and all equipment assigned to employees or students must be returned prior to leaving their position or school. All equipment containing sensitive information and data must be returned directly to WPS before it can be redeployed.

Personal Electronic Devices:

The use of personal electronic devices is permitted at the discretion of the Principal and Director of Educational Technology. The WPS is not responsible for the maintenance and security of personal electronic devices and assumes no responsibility for loss or theft. The district reserves the right to enforce security measures on personal devices when used to access district tools and remove devices found to be in violation of the AUP.

Energy Management:

WPS strives to reduce our environmental footprint by pursuing energy conservation efforts and practices. The district reserves the right to adjust power-saving settings on electronics to reduce the energy consumption.

Technology Purchasing & Donations:

Technology hardware and software must be purchased or donated through WPS unless prior approval has been received by WPS and the Business Office. All technology purchases and donations must abide by City procurement policies and are subject to approval by WPS. Technology pricing can include additional expenses required to ensure proper maintenance and security, including but not limited to warranties, hardware/software upgrades, virus protection, and security/inventory software. Schools or departments applying for technology grants, funding, or donations must budget for any additional expenses associated with the requested technology and can be held responsible for any additional expenses incurred.

AUP POLICY REVIEW:
Reviewed and approved: This policy will be reviewed annually by the WPS Office of the Legal

Advisor, WPS Educational Technology, and the Superintendent's Office.

Distribution: District's Website and Student, Employee and Substitute Handbooks

Revision: Requests for AUP amendments can be forwarded to the Director of Educational Technology.