Boston Public Schools

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

ACCEPTABLE USE POLICY AND GUIDELINES

Scope of Policy

Boston Public Schools (BPS) 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 central offices to increase community engagement, staff and student learning, and core operational efficiency.
- BPS has a legal and moral obligation to protect the personal data of our students, families, and staff.
- BPS 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, families, 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 BPS Chief Information Officer and is issued via the Superintendent's Circular. 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 Boston Public Schools for Families & 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 BPS technology resources is a privilege, not a right. By using BPS Internet Systems and devices, the user agrees to follow all BPS regulations, policies and guidelines. Students and staff are required to report misuse or breach of protocols to appropriate personnel, including building administrators, direct supervisors and to the Office of Instructional and Information Technology (OIIT). 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.
- 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 Boston Public Schools for

electronic documents/communications stored or transmitted through district systems unless that information could be detrimental to governmental or personal interests. For more infomation, 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 families of the Boston Public Schools. Personal information stored or transmitted by agents of the Boston Public Schools must abide by FERPA laws and the BPS 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

Children's Internet Protection Act (CIPA) - Requires schools that receive federal funding through the E-Rate program to protect students from content deemed harmful or inappropriate. The Boston Public Schools is required to filter internet access for inappropriate content, monitor the internet usage of minors, and provide education to students and staff on safe and appropriate online behavior.

Communication & Social Media

Employees and students are provided with district email accounts and online tools to improve the efficiency and effectiveness of communication, both within the organization and with the broader community. Communication should be consistent with professional practices used for all correspondence. When using online tools, members of the BPS community will use appropriate behavior:

a) when acting as a representative or employee of the Boston Public Schools.
b) when the communication impacts or is likely to impact the classroom or working environment in the Boston Public Schools.

All communication sent by an employee using district property or regarding district business could be subjected to public access requests submitted through Freedom of Information Act (FOIA). Users need to be aware that data and other material/files maintained on the school district's systems may be subject to review, disclosure, or discovery. Use of personal email accounts and communication tools to conduct school business is strongly discouraged and may open an individual's personal account to be subject to FOIA inquiries. BPS will cooperate fully 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

· Communication with students should not include content of a personal nature.
· 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.
· When communicating with a parent/guardian, refrain from discussing any non-related students.
· Employees who use internal or external social media (blogs, Twitter, etc.) are expected to maintain professionalism at all times. This includes refraining 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.
· When using social media, employees are expected to refrain from posting any negative comments online about students or colleagues.
· Employees are required to notify their principal/headmaster before setting up an online site to facilitate student learning. Employees are responsible for monitoring all communication on the site to ensure a safe learning environment.
· Employees are advised not to add any students/former students or parents as 'friends' or contacts on social media unless the site is specifically set up to support classroom instruction or school business.
· Employees may communicate with BPS graduates (+18 years old) on social media but should be advised to maintain professionalism and caution when communicating online.
· Employees are advised not to add parents/guardians of students as 'friends' or contacts on social media to maintain professionalism and to avoid any appearance of conflict of interest.
· Avoid responding to spam or phishing attempts that require a user to click on any links or to provide any account information. Note: BPS 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 OIIT Help Desk (617-635-9200)

Solicitation

Web announcements and online communication promoting a business are prohibited by the BPS 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 BPS network or other resources are prohibited and have the potential to create liability for the district as well as for the individual. BPS staff and students must comply with regulations on copyright plagiarism that govern the use of material accessed through the BPS 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. BPS will cooperate with copyright protection agencies investigating copyright infringement by users of the computer systems and network of the Boston Public Schools.

Network Usage

Network access and bandwidth is provided to schools for academic and operational services. BPS 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 BPS network to access content deemed 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), BPS is required to protect students from online threats, block access to inappropriate content, and monitor Internet use by minors on school networks. OIIT is responsible for managing the district's Internet filter and will work with the BPS community to ensure the filter meets the academic and operational needs of each school while protecting minors from inappropriate content.

By authorizing use of technology resources, BPS 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 BPS network or in BPS systems. BPS reserves the right to access, review, copy, store, or delete any files stored on BPS computers and all employee and students communication using the BPS network. Electronic messages and files stored on BPS computers or transmitted using BPS 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. BPS may choose to deploy location tracking software on devices for the sole purpose of locating devices identified as lost or stolen.

Personal Use

BPS recognizes that users may use BPS 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 BPS 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 OIIT 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 Chief Information Officer.

Data & Systems

Access to view, edit, or share personal data on students and employees maintained by BPS 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-BPS individuals requesting protected data must receive approval from the Office of the Legal Advisor and have a non-disclosure agreement with the BPS. Individuals requesting ongoing access to data through BPS systems are required to have a designated BPS 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 BPS 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 Boston Public Schools and the City of Boston 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 OIIT. Users are encouraged to use BPS approved data/information systems for the storage and transmission of sensitive data whenever possible and avoid storage on local hardware that can not be secured.

Electronic Devices

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

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

Device Support

BPS provides basic installation, synchronization, and software support for BPS-issued electronic devices. Devices must be connected to the BPS network on a regular basis to receive an up-to-date software and antivirus updates and for inventory purposes. Password protection is required on all BPS-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 OIIT Service Desk (617-635-9200). The BPS 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 BPS 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 OIIT before it can be redeployed.

Personal Electronic Devices

The use of personal electronic devices is permitted at the discretion of the Principal/Headmaster and Chief Information Officer. The BPS 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

BPS 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 OIIT unless prior approval has been received by OIIT and the Business Office. All technology purchases and donations must abide by City procurement policies and are subject to approval by OIIT. 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 BPS Office of the Legal Advisor, OIIT, and the Superintendent's Office.
Distribution: Superintendent's Circular, Office of Human Capital, Office of Instructional and Information Technology and posted on District's web site and Boston Educator Development and Feedback System.
Revision: Requests for AUP amendments can be forwarded to BPS Chief Information Officer.

I have read and accept the conditions stated above.

Name:_____ Date:_____

Signature:_____

Boston Public Schools
Acceptable Use Policy for Networks
BPS Staff

It is the policy of the Boston Public Schools that all students and staff will use all technology to access electronic ("computer") networks including the Internet and email, in a responsible, legal and ethical manner. Failure to do so may result in the termination of network and e-mail privileges for the user or prosecution under federal or state law.

Since network communication is often public, staff are responsible for behaving appropriately on the BPS network and for using the BPS network only for educational and professional purposes. The network is provided for students and staff to conduct research and communicate with others professionally.

Individual users of the network are responsible for their use of the network. Use of the network for any illegal or commercial activities is prohibited.

The BPS uses a filtering system for all schools, and for central offices. This filtering system is designed to prevent access to educationally inappropriate sites. However, it is important to understand that no solution is perfect, and at times educational sites may be incorrectly blocked and conversely, inappropriate sites may not be blocked. Employees who are using the Internet as part of their teaching should be aware that they may call the BPS Technology Help Desk (635-9200) to request that a specific site be blocked or un-blocked. Such decisions will be made by those responsible for monitoring the filtering service within the BPS. Please also note that our filtering system **allows us to track and monitor all computer use on the network.**

A responsible network user will:

- Use language that is considered appropriate.
- Be polite.
- Send information that other users will not find offensive.
- Conform with copyright laws and always give credit to the author of the material used.
- Never reveal personal information about any user such as address, telephone number, credit card numbers, social security number, etc.
- Neither tamper with the system nor alter, delete or destroy any files or data that are not yours.

A responsible network user must be aware that:

- Use of the network and e-mail is a PRIVILEGE, not a RIGHT.
- **The BPS network is to be used only for educational purposes**
- E-mail is not guaranteed to be private.
- Identifying photos of students with their first and last names may not be used on a web site.
- It is important to log off the computer at the end of every session, so another user can not use your password.
- Violation of this policy will result in the possible loss of Internet privileges and/or disciplinary action pursuant to the Code of Discipline and/or prosecution under state and federal law.
- Persons issued an account are responsible for its use at all times.

I have read and accept the conditions stated above.

Name:_____ Date:_____

Signature:_____