BURLINGTON
PUBLIC SCHOOLS

Technology Responsible Use Policy

Introduction

This Technology Responsible Use Policy (RUP) for the Burlington Public Schools (BPS) is enacted by the School Committee to provide the parents, students, and staff of the Burlington School Community with a statement of purpose and explanation of the use of technology within the Burlington learning community. This policy is reinforced by practice, acceptable use standards and is required to be read before accessing the technology devices, digital resources, and network infrastructure of the Burlington Public Schools.

Purpose

The Burlington Public Schools encourage the use of technology to assist staff and students with academic success, preparation for the workplace, and lifelong learning. The Burlington Public Schools provides access to a wide range of technology to support learning and communicating with others. Technology will be used to increase communication, enhance student engagement, and assist staff and students in acquiring new skills. The technology devices, digital resources, and network infrastructure will also be utilized to provide relevant school information to a global community.

The purpose of the Burlington Public Schools (BPS) Responsible Use Policy is to prevent unauthorized access and other harmful or unlawful activities by users online, prevent unauthorized disclosure of or access to sensitive information, and to comply with legislation including, but not limited to, the Children's Internet Protection Act (CIPA), Children's Online Privacy Protection Act (COPPA) and Family Educational Rights and Privacy Act (FERPA).

BPS uses technology protection measures to block or filter access, as much as reasonably possible, to visual and written depictions that are obscene or harmful to minors over the network. The District can and will monitor students' online activities and access, review, copy, and store or delete any communications or files and share them with adults as necessary. Students should have no expectation of privacy regarding their use of BPS equipment, network, and/or Internet access or files, including email.

Google Workspace for Education accounts are provided to all students and staff. BPS provides students with a closed-campus email account. Email usage may be monitored and there is no expectation of privacy with school email accounts. Email accounts issued to students are archived to ensure student safety. BPS will take all necessary measures to secure the network against potential cyber security threats. This may include blocking access to websites, applications, including, but not limited to, email, data management and reporting tools, and other web applications.

This RUP is in effect when BPS provided equipment is used on or off school property and/or when non BPS devices access the BPS district network or district resources; or, at home, or other locations, if the improper use creates a hostile environment at school for any student/employee and/or causes disruption or disorder within the school.

Parental Permission

The student use of BPS devices and applications is verified via this Responsible Use Policy and/or inclusion of the RUP in the school Student Handbook. Please reach out to your child's teacher or school administration with any questions or concerns or to discuss opting out of the use of any applications. All apps are reviewed and vetted for approval based on the strict requirements of the Student Data Privacy Consortium (see below for details).

Summary

Burlington Public Schools believes in a Digital Citizenship model for supporting safe and responsible use of all technology and web based communication in teaching and learning. An important part of this is that we are able to show others what that responsible use looks like. Because we know this is important for us all, we ask everyone, the staff, students and volunteers working at our schools to agree to use these technologies in a safe and responsible way.

All are responsible for practicing positive Digital Citizenship. Positive Digital Citizenship includes appropriate behavior and contributions on websites, social media, discussion boards, media sharing sites and all other electronic communications. It is important to be honest in all digital communications without disclosing sensitive personal information. Students should also reference the student handbook for additional policies and guidelines.

Burlington Public Schools provides filtered network and wifi access for all users. Students and staff should only be accessing the BPS wifi. The BPS Guest wifi is available only to guests, visitors, and contracted providers requiring access to wifi while at Burlington Public Schools. Students and staff should not be connected to or accessing the Guest wifi.

Definitions

"Technology devices, digital resources, and network infrastructure" is defined as the Burlington Public Schools network, the Internet, Google Workspace, email, hardware, software, printers, peripheral devices, individual computer devices, and web enabled devices.

"Information technology" is defined as Internet access, blogging, podcasting, email, published and unpublished documents, and various forms of multimedia technology.

"Educational use" is defined as a use that supports communication, research, and learning.

"Devices" refer to district owned/leased, staff owned devices, and student owned devices.

Children's Online Privacy Protection Act (COPPA)

Congress enacted the Children's Online Privacy Protection Act, 15 U.S.C. §6501, et seq. (COPPA) in 1998. COPPA required the Federal Trade Commission to issue and enforce regulations concerning children's online privacy. The Commission's original COPPA Rule became effective on April 21, 2000. The Commission issued an amended Rule on December 19, 2012 that became effective on July 1, 2013.

Burlington Public Schools works diligently to comply with COPPA requirements. Burlington Public Schools does not collect student personal information or transmit such information directly to online entities for the purpose of creating web based accounts. In cases of web based account creation, Burlington Public Schools will use an internal school district identification number to represent each student user.

Consequences for Irresponsible Use

Misuse of BPS devices and/or technology of any kind may result in restricted access. Such misuse may also lead to disciplinary and/or legal action, including suspension, expulsion, or criminal prosecution by government authorities. The District will handle any disciplinary action to the specific issues related to each violation.

Disciplinary action may also be taken when a student intentionally directs at the school online speech that is understood by school officials to threaten, harass and intimate a staff member or fellow student, even when such online action originated, and was disseminated, off-campus without the use of school resources.

Implementation of this Policy

The Superintendent of Schools or his/her designee(s), shall develop and implement administrative regulations, procedures, terms and conditions for use and user agreements consistent with the purposes and mission of the Burlington Public Schools as well as with applicable laws and this policy.

What are Google Apps and Google Workspace for Education?

Burlington Public Schools provides staff and students with a Google Workspace for Education account. Google Workspace is a web based suite of programs provided by Google for schools to use. All staff and students in Burlington Public Schools have access to Google Workspace.

All of the Google Workspace services can be accessed from anywhere you have an Internet connection (school, home, smart phone, etc.) Google Workspace allows you to easily share documents and files with teachers and other students, so you can turn in assignments electronically and collaborate on projects with classmates.

Burlington Public Schools Student Google Account Setup

BPS student accounts are created using only student local identification numbers. The student's username is their local student ID - such as 123456

Google Workspace accounts include the following applications:

- Google Gmail - student and staff email accounts
- Google Drive - unlimited cloud based data storage and management
- Google Classroom - cloud based learning management solution
- Google Documents - cloud based word processor similar to Microsoft Word
- Google Slides - cloud based multimedia presentation tool similar to PowerPoint
- Google Sheets - cloud based spreadsheet program similar to Microsoft Excel
- Google Forms - cloud based survey/data collection tool
- Google Meet - video conferencing and communication tool

BPS user access settings restrict student Gmail for communication with staff and students only within the

Burlington Public Schools domain.

Data storage is provided via Google Drive. Google Drive can be accessed from any computer with an Internet connection. Google Drive allows users to access and share files from any device that has Internet connectivity.

Use of Google Meet for Video Conferencing Statement of Responsibility:
Google Meet (video conferencing) provides video conferencing in remote learning situations and for meetings. When we utilize video communication, it is important that we continue to respect the privacy and intellectual property rights of our teachers and our students. By participating in the use of video conferencing, you agree that you may not save, record, share, or post this session or any photos from any video session. I also agree that I will not save, record, share or post this session or any photos from any video session. Please note that Massachusetts Law makes it a crime to secretly record a conversation, whether the conversation is in-person or taking place by telephone or another medium.

Uses for Student Gmail

Email can be a powerful communication tool for students to increase communication and collaboration. Students are encouraged to check their email at least once per day. Teachers may send email to middle and high school students to communicate reminders, course content, pose questions related to class work, and assignments. Several applications including Google Classroom use email as a notification service. Students may send email to their teachers with questions or comments regarding class. Students may send email to other students to collaborate on group projects and assist with school classes.

Student Gmail Permissions

Burlington Public Schools' Gmail system controls who email messages can be sent to and who they can be received from. BPS Students cannot send email to parent accounts or anyone outside of the Burlington Public Schools domain. All BPS students cannot receive email from outside of the domain. Therefore, students should not use their BPS email for setting up accounts that need to be verified via email or receive notices via email.

Student Emails to Staff

Students are encouraged to email staff concerning school-related content and questions. However, there will be no requirement or expectation for staff to answer student email outside of their regular work day, although they certainly may if they choose. For example, an unanswered email to a teacher would not excuse a student from turning in an assignment.

General Email or Chat Guidelines

Below is a general summary of guidelines related to email, on-line chat, or instant messages:

- Email and on-line chat is to be used for school-related communication.
- Do not send harassing email or instant messages or content.
- Do not send offensive email or instant messages or content.
- Do not send spam email or instant messages or content.
- Do not send email or instant messages containing a virus or other malicious content.
- Do not send or read email or instant messages at inappropriate times, such as during class instruction.
- Do not send email or instant messages to share test answers or promote cheating in any way.
- Do not use the account of another person.

Approved Apps and Sites - Student and Staff Data Privacy

Burlington Public Schools is committed to providing safe online environments for students and staff. We are committed to developing practices that protect data privacy for all users. In an effort to improve those practices, we have joined The Education Collaborative's (TEC) Student Data Privacy Alliance.

Data collection is essential for improving academic achievement in today's modern digital learning environments, since data is pivotal in measuring student progress to steer personalized learning decisions. While recognizing the importance of real-time data in guiding student success, school officials also acknowledge their roles as gatekeepers. As a school district, we have a moral and ethical duty to ensure that our students' information is protected while using any online digital tools for learning. While technology may make accessing student data relatively easy, it needs to be maintained securely and confidentially, and that is a responsibility we take very seriously. Our partnership with TEC's Student Data Privacy Alliance is vital to our district's student data privacy efforts.

BPS utilizes TEC's Student Data Privacy Alliance (SDPA) administrative and legal support to negotiate privacy terms with our software vendors. TEC's service was launched in 2017 in response to the needs of its member districts. In cooperation with the Student Data Privacy Consortium, TEC developed a statewide Data Privacy Agreement (DPA) that now spans 5 states: Massachusetts, New Hampshire, Rhode Island, Maine, and Vermont. These legally enforceable documents articulate a vendor's responsibilities and the duties required to protect student data in compliance with all applicable federal and state privacy statutes, including FERPA, PPRA, COPPA. TEC now services over 240 school districts with expert legal counsel and experienced contract administrators. To date, they have achieved over 1700 signed vendor agreements.

Please see our Burlington Public Schools TEC SDPA site with information about approved apps and websites.

Content Filtering
The Burlington Public Schools use applications designed to block access to certain sites and filter content as required by the Children's Internet Protection Act, 47 U.S.C. §254 (CIPA). Burlington Public Schools is aware that not all inappropriate information can be filtered and the district will make an effort to correct any known gaps in the filtering of information without unduly inhibiting the educational use of age appropriate content by staff and students. Users will inform teachers or administrators of any inadvertent access to inappropriate material, in order that there is appropriate modification of the filtering profile. Burlington Public Schools educates students about appropriate online behavior, including interacting with other individuals on social networking Web sites and in chat rooms and cyber bullying awareness and response.

Monitoring
The Burlington Public Schools monitors the use of the school department's network to protect the integrity and optimal operation of all computer and system networks. There is no expectation of privacy related to information stored and transmitted over the Burlington Public Schools network. The information on the network in general files and email is not private and is subject to review by the network manager at the request of the Burlington Public Schools administration to substantiate inappropriate activity and to comply with requests of law enforcement agencies as part of their investigations.

The Burlington Public Schools will cooperate with copyright protection agencies investigating copyright infringement by users of the computer systems and network of the Burlington Public Schools.

Technicians and computer system administrators maintain full access rights to all storage devices, and may need to access/manage such storage devices as part of their duties.

Routine maintenance and monitoring of the system may lead to discovery that a user has or is violating the Burlington Public Schools Responsible Use Policy, other school committee policies, state laws, or federal laws.

Search of particular files of a user shall be conducted if there is a reasonable suspicion that a user has violated the law or Burlington School Committee Policies. The investigation will be reasonable and in the context of the nature of the alleged policy violation.

Email that is sent within the BPS district is monitored and filtered based upon content. Rules/filters are set up to monitor student email for profanity, harassment, and other inappropriate content. Student email that is identified as inappropriate will be reviewed by the school administration.

User Access and Explanation of Guideline

Access to information technology through the Burlington Public Schools is a privilege, not a right. Students, parents, and staff shall be required to read the BPS Responsible Use Policy.

The BPS RUP shall govern all use of technology devices, digital resources, and network infrastructure. Student use of technology resources, digital resources, web enabled devices, and network infrastructure will be governed by the Burlington School committee disciplinary policies as outlined in the policy manual of the district and the student's school handbook.

Because information technology is constantly changing, not all circumstances can be anticipated or addressed in this policy. All users are expected to understand and comply with both the "letter" and the "spirit" of this policy and show good judgment in their use of these resources.

The Burlington Public Schools provides students access to its technology devices, digital resources, and network infrastructure, along with information technology for educational use. If a student has doubts regarding whether a resource has educational merit, he/she should ask a staff member.

Scope of Technology Policies

Policies, guidelines and rules refer to all computing devices including but not limited to computers, mobile web enabled devices, iPads, portable memory storage devices, calculators with interfacing capability, cell phones or ECDs (electronic communication devices), digital cameras, etc., as well as technology infrastructure, associated peripheral devices and/or software.

Policies, guidelines, and rules refer to any computing or telecommunication devices owned by, leased by, in the possession of, or being used by students and/or staff that are operated on the grounds of any district facility or connected to any equipment at any district facility by means of web connection, direct connection, telephone line or other common carrier or any type of connection including both hardwired, fiber, infrared and/or wireless.

This RUP also applies to any online service provided directly or indirectly by the district for student use, including but not limited to: Google Workspace accounts, Email, Calendar, and Aspen (Parent/Student Access to Student Information System).

Expectation of Privacy

At any time and without prior notice, the BPS reserves the right to monitor, inspect, copy, review, and store any and all usage of technology devices, digital resources, and network infrastructure, along with information technology as well as any information sent or received in connection with this usage. Staff and students should not have any expectation of privacy regarding such materials.

Consequences for Violation of Technology Policies

Use of the computer network and Internet is an integral part of research and class work, but abuse of this technology can result in loss of privileges. Students who use technology devices, digital resources, and network infrastructure, along with information technology inappropriately may lose their access privileges and may face additional disciplinary or legal action. The length of time for loss of privileges will be determined by building administrators and/or other staff members. If the user is responsible for multiple violations, privileges can be removed for one year or more.

Unacceptable Uses of Technology Resources
Inappropriate technology use includes but is not limited to the following:

- Interfering with the normal functioning of devices, computer systems, or computer networks.
- Damaging or theft of devices, computer systems, or computer networks.
- Accessing, modifying, or deleting files/data that do not belong to you.
- Sending or publishing offensive or harassing messages and content.
- Accessing dangerous information that, if acted upon, could cause damage or danger to others.
- Giving your username or password to any other student, or using the username or password of someone else to access any part of the system. Sharing and/or distribution of passwords or using another student or faculty member’s password. Intentional viewing, downloading or distribution of inappropriate and/or offensive materials.
- Gaining unauthorized access to computer and or telecommunications networks and resources.
- Viewing, transmitting or downloading pornographic, obscene, vulgar and/or indecent materials.
- Using obscene language, harassing, insulting or bullying others, posting of private or personal information about another person, spamming of the school email system, violating any federal or state law, local regulation or school committee policy.
- Violating copyright laws and/or the district policy on plagiarism. Copying software or applications from Burlington Public School devices through any electronic means unless the particular licensing agreement in place for the software allows user distribution.
- Intentionally wasting limited network or bandwidth resources. Destructions/vandalism of system software, applications, files or other network resources Employing the network for commercial or political purposes. Using the network / Internet to buy or sell products.
- “Hacking” and other illegal activities in an attempt to gain unauthorized access to restricted files, other devices or computer systems. Uploading any harmful form of programming, bypassing filters; installing any type of server, aliasing / spoofing, peer-to-peer networking or remote-control software.
- Possession of and/or distribution of any of software tools designed to facilitate any of the above actions will also be considered an offense.
- Saving inappropriate files to any part of the system, including but not limited to:

    Music files
    Movies
    Video games of all types, including ROMs and emulators
    Offensive images or files
    Programs which can be used for malicious purposes
    Any files for which you do not have a legal license
    Any file which is not needed for school purposes or a class assignment

Uses that contribute to the violation of any other student conduct code including but not limited to cheating, plagiarism, hazing or harassment, theft, falsification of records, possession of banned substances/items, etc.

NOTE: If you need a file for a class project that you think may be considered inappropriate, then you need to have teacher and school administration permission prior to the class project.

Due Process
The Burlington Public Schools will apply progressive discipline for violations of the district policy which may include revocation of the privilege of a user's access to technology devices, digital resources, and network infrastructure, along with information technology. Other appropriate disciplinary or legal action may be undertaken by the Burlington Public Schools administration. The nature of the investigation will be reasonable, and for staff, will reflect the contract language for each bargaining unit.

Disclaimer
BPS makes no guarantees about the quality of the services provided and is not liable for any claims, losses, damages, costs, or other obligations arising from use of the network or district accounts. BPS also denies any liability for the accuracy or quality of the information obtained through user access. Any statement accessible online is understood to be the author's individual point of view and not that of the district, its affiliates, or employees. Parents or legal guardians should supervise the usage of BPS network accounts outside of school. The student's parent or guardian is responsible for monitoring the minor's use outside of school.

Burlington Public Schools Limitations of Liability
The Burlington Public Schools makes no warranties of any kind, implied or expressed, that the services and functions provided through the Burlington Public Schools technology devices, digital resources and network infrastructure, along with information technology will be error free or without defect. The Burlington Public Schools will not be responsible for damages users may suffer, including but not limited to loss of data or interruption of service.

The Burlington Public Schools, along with any persons or organizations associated with the school department internet connectivity, will not be liable for the actions of anyone connecting to the internet through the school network infrastructure. All users shall assume full liability, legal, financial or otherwise for their actions while connected to the internet.

The Burlington Public Schools assumes no responsibility for any information or materials transferred or accessed from the internet.

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

Parents and guardians agree to accept financial responsibility for any expenses or damages incurred as a result of their student's inappropriate or illegal activities on the Burlington Public Schools network. Parents and guardians agree to reimburse Burlington Public Schools for any expenses or damages incurred in the use of district owned devices such as iPads in 1:1 school deployments. Parents and guardians will have access to optional third party insurance carriers.

Modification
The Burlington School Committee reserves the right to modify or change this policy and related implementation procedures at any time. Prior to implementation for staff, presidents of each of the bargaining units will be notified.

BURLINGTON
PUBLIC SCHOOLS

Responsible Use Statement
Middle and High School Students

By reading this Responsible Use Policy I acknowledge that I understand the following:

- I am responsible for practicing positive digital citizenship including appropriate behavior and contributions on websites, social media, discussion boards, sharing sites, and all other electronic communications.
- I am responsible for treating others with respect and dignity. I will not send and/or distribute hateful, discriminatory, or harassing digital communications of any kind. I understand that bullying in any form, including cyber bullying, is unacceptable.
- I am responsible for keeping personal information private. I will not share personal information about myself or others including, but not limited to, names, home addresses, telephone numbers, birth dates, or visuals such as pictures, videos, and drawings. I will be aware of privacy settings on websites that I visit.
- I will abide by all laws, this Responsible Use Policy, and all District guidelines set by school Student Handbooks. I understand that what I do and post online must not disrupt school activities or compromise school safety and security. I understand that the use of the District network for illegal, political, or commercial purposes is strictly forbidden.
- I am responsible for my passwords and my actions when using District accounts. I will not share any school or district usernames and passwords with anyone. I will not access the account information of others.
- I am responsible for my verbal, written, and artistic expression. I will use school appropriate language in all electronic communications, including email, social media posts, audio recordings, video conferencing, and artistic works.
- I am responsible for accessing only educational content when using BPS technology. I will not seek out, display, or circulate material that is hate speech, explicit, or violent. I understand that any exceptions must be approved by a teacher or administrator as part of a school assignment.
- I am responsible for respecting and maintaining the security of BPS digital resources and networks. I will not try to get around security settings and filters, including through the use of proxy servers or VPNs to access websites blocked by the district. I will not install or use illegal software or files, including copyright protected materials, unauthorized software, or apps on any BPS devices.
- I will not use the BPS network or equipment to obtain unauthorized information, attempt to access information protected by privacy laws, or impersonate other users.
- I am responsible for taking all reasonable care when handling BPS equipment. I understand that vandalism in any form is prohibited. I will respect my and others' use and access to BPS equipment.

- I am responsible for respecting the works of others. I will follow all copyright guidelines. I will not copy the work of another person and represent it as my own and I will properly cite all sources. I will not download illegally obtained music, software, apps, and other works. I understand all BPS trademarks, logos and symbols are for school district use only.
- I am responsible for the data I create and for protecting it. I understand the district provides me with a Google account to save and store all my data and files. I understand it is my responsibility to backup and protect any data or files that I create.
- I know that the conduct that is forbidden in school is also forbidden when I use computers outside of school if it interferes with other students' education, and if I break the rules there will be consequences in school.

Video Conferencing Responsible Use Statement

Google Meet (video conferencing) provides video conferencing in remote learning situations and for meetings. When we utilize video communication, it is important that we continue to respect the privacy and intellectual property rights of our teachers and our students. By participating in the use of video conferencing, you agree that you may not save, record, share, or post this session or any photos from any video session. I also agree that I will not save, record, share or post this session or any photos from any video session. Please note that Massachusetts Law makes it a crime to secretly record a conversation, whether the conversation is in-person or taking place by telephone or another medium.

BURLINGTON
PUBLIC SCHOOLS

Responsible Use Statement
Elementary School Students

As a part of my schoolwork, my school provides me with the use of iPads and other technology devices. I understand that the use of all technology is a privilege. My behavior and language are to follow the same rules I follow in my class and in my school. My school gives me an iPad to use for learning. When using my iPad, my words and behavior should be kind and appropriate.

To help myself and others, I agree to the following:

- I will use school technology only with a teacher's permission.
- I will use school technology only to do school work, whether at school or outside of school, and not for any other reason.
- I will not create or store material that is not related to my schoolwork.
- I will not share my password with anyone other than my teacher or parent/guardian, and I will not ask for or use anyone else's password.
- I will practice online safety and not use school technology to share my address or telephone number, or any other personal information about myself or anyone else.
- I will not upload, link, or embed an image of myself or others without my teacher's permission.
- I will not create or use images of others without my teacher's permission.
- I will be polite, considerate, and use appropriate language when I use school technology; I will not use it to annoy, be mean to frighten, threaten, tease, or bully; I will not use inappropriate words or any other rude language.
- I will not try to see, send, or upload anything that says and/or shows bad or mean things about anyone's race, religion, or gender.
- I agree to tell an adult if I read, see, or access something inappropriate or if I witness inappropriate use of technology.
- I will respect the work of others and not take credit for other people's work.
- I will not access another student's files and folders without their permission.
- I will only share my own files and folders when asked by my teacher.
- I will treat school technology with care and protect it from damage.
- If I have or see a problem with school technology, I will tell the teacher.
- I will allow teachers to look at my work to be sure that I am following these rules, and if I am not, there will be consequences which may include not being able to use technology.
- I know that the conduct that is forbidden in school is also forbidden when I use computers outside of school if it interferes with other students' education, and if I break the rules there will be consequences in school.
- I will only use websites and apps that are approved by teachers.

Video Conferencing Responsible Use Statement

Google Meet (video conferencing) provides video conferencing in remote learning situations and for meetings. When we utilize video communication, it is important that we continue to respect the privacy and intellectual property rights of our teachers and our students. By participating in the use of video conferencing, you agree that you may not save, record, share, or post this session or any photos from any video session. I also agree that I will not save, record, share or post this session or any photos from any video session. Please note that Massachusetts Law makes it a crime to secretly record a conversation, whether the conversation is in-person or taking place by telephone or another medium.

BURLINGTON
PUBLIC SCHOOLS

Bring Your Own Device Responsible Use Policy

The Burlington Public Schools (BPS) Bring Your Own Device (BYOD) Responsible Use Policy (RUP) is part of the School District and Town of Burlington Information Security Program.

Information security policies are the principles that direct managerial decision-making and facilitate secure business operations. A concise set of security policies enables the BPS IT Team to manage the security of information assets and maintain accountability. These policies provide the security framework upon which all subsequent security efforts will be based. They define the appropriate and authorized behavior for personnel approved to use information assets, such as laptops, tablets and smartphones. Policies are the organizational mechanism used to manage the confidentiality, integrity and availability issues associated with information assets. Information assets are defined as any information system (hardware or software), data, networks, and components owned or leased by or its designated representatives.

BPS BYOD Responsible Use Policy
This policy provides guidelines for using personally owned devices and related software for educational, medical or municipal use. The BYOD RUP applies to all employees, students, contractors, vendors and any other person using or accessing the School District or Town Municipal network. Exceptions to this policy must be approved by the IT/MIS department. Furthermore, based on the amount of personally identifiable information (PII) employees work with, management reserves the right to determine which employees can use personally owned devices and which cannot. General Policy recognizes that personally owned equipment can play a valuable role in convenience, efficiency and productivity of its employees. Nonetheless, the use of these devices must be monitored closely. All personally-owned devices must be registered with the IT department in advance.

The following is a list of personally owned devices permitted for educational, student medical, or municipal use:

- Desktop computers
- Laptop computers
- Tablets
- Internet enabled phones
- Personal digital assistants (PDAs)

End-User Support
Users of personally owned devices will not use or request IT resources including troubleshooting issues related to network connectivity, installation of equipment, or software. Users are responsible for learning, administering, installing and setting up their personally owned devices.

The user should follow good security practices including:

- Password protecting all personally owned devices
- Updating to the latest version of their operating system and installing antivirus and/or malware protection software
- Being vigilant of your device so as to not leave any owned devices unattended. Release of Liability and Disclaimer to Users hereby acknowledges that the use of personally owned devices in connection with business carries specific risks for which you, as the end user, assume full liability. In the case of litigation, may take and confiscate a user's personally owned device at any time.

General Policy Users that wish to access the network using their personally owned computer may do so using only authorized software and only with the approval of the user's supervisor and the IT department. Users must follow the same rules when accessing the network from both school/town issued equipment and personally owned devices.

When connected to the network, the user will NOT:

- Use the service as part of violating the law
- Attempt to break the security of any computer network or user
- Attempt to send a massive amount of email including junk or spam to a specific person or system in order to flood their server

Authorization of Devices
IT reserves the right to determine the level of network access for each personally owned device.

Students Requesting Access to the Network Using their Personal Device for Medical Necessity

Students requesting access to the network for medical reasons, with their personal device to the network, must have the approval from the nurse's office at the school that the student is attending, and the request must be submitted by the nurse in charge. A parent or guardian must complete the **Form for BPS Personal Medical Device/Phone Access to Network** prior to a student device being allowed on the BPS Wifi network.

BURLINGTON PUBLIC SCHOOLS

Responsible Use Policy
Burlington Public Schools Staff
BPS Issued Devices (Laptops, iPads, Peripherals)

Burlington Public Schools provides staff members with appropriate instructional/work devices. These devices may include laptop computers, iPads, peripherals, projectors, cameras, printers, robotics, and multimedia equipment. Staff members will use these devices in accordance with the Burlington Public Schools Responsible Use Policy. All devices are property of Burlington Public Schools.

- All BPS issued staff devices are work devices and as such will be used for work related tasks.
- Care of these devices is critical to sustain devices and support the district's ability to provide devices on a regular refresh cycle.
- Report any breakage or loss to the BPS IT Department.
- **Do not** personalize equipment with stickers, labels, or markings that are not provided by the BPS IT Department.
- **Do not** remove, tamper, or adjust security profiles and restrictions to BPS issued staff devices.
- **Laptops will be replaced every 5 years based on the availability and funding and subject to change.**
- iPads issued to appropriate staff members will be replaced on an iOS cycle according to need.
- The iPad replacement cycle is based on the availability of district budgets and funding and subject to change.
- If it is determined that a staff member's intentional act has damaged, destroyed, or lost any device, the staff member assumes full financial responsibility.
- **Staff members must return all devices and peripherals immediately to the school's main office or the IT Department upon any change in position.** This includes new appointments within the Burlington Public Schools, leave of absence, resignation, retirement, or termination.

BURLINGTON
PUBLIC SCHOOLS

iPad 1:1 Learning Program for Grades 6-12
Student and Parent/Guardian Statement of Responsibility

We have read, understand, and will follow this Statement of Responsibility. We recognize that technology access is provided for educational purposes in keeping with the academic goals of Burlington Public Schools.

- We understand that all technology devices are the property of the Burlington Public Schools and BPS reserves the right to specify the immediate return of the equipment at any time.
- We understand that if the student breaks this agreement, the consequences could include suspension of technology privileges including take home access and/or disciplinary action according to the Burlington Public Schools Technology Responsible Use Policy and/or School Student Handbook.
- We understand that the BPS school network and BPS Google Workspace accounts are owned and managed by BPS and that BPS has the right to access any of the information created, shared, or communicated through these systems at any time.
- We agree to return the iPad to Burlington Public Schools in good working condition with the charging cord and the keyboard case on a date specified by the school district.
- We understand that the assigned iPad should be brought to school with a fully charged battery each day.
- We understand that loaner iPads are only available for use when the assigned iPad is broken or damaged and that the RUP applies to the use of any loaner devices. Use of loaner devices will be monitored for consecutive days of borrowing to ensure that assigned device is not damaged or lost. Loaner devices must stay at school.
- We understand that the iPad is supervised by BPS and will have restrictions enabled for the Apple App Store. We understand that these restrictions can't be removed and opting out is not available.
- We understand that the iPad will not be filtered while accessing the Internet off of the school network.
- We will discuss different ways in which the student can communicate online with other people using devices and what safe, responsible, and respectful digital communication looks like.

Accidental damage to iPads will be covered by the district's iPad Care Program

- **Student/Parent/Guardian will be responsible for a $50 deductible upon *every* accidental damage incident.**
- Deductible can be paid via Check only made out to Burlington Public Schools
- Students must report any damage or loss of iPad to their homeroom teacher
- Homeroom teacher will place a technology support ticket for the damaged or lost iPad
- BPS IT Team will replace the damaged iPad (if deemed accidental)
- **BPS will no longer be offering an optional insurance program for iPads so there is no need to sign up for iPad insurance. Do not fix or replace the iPad on your own.**

We understand that we are accepting full financial responsibility ($400) for any destruction or vandalism of an iPad and keyboard case deemed malicious by the school district as well as loss of the device.

What do we need to do now?

- **Families don't need to do anything right now**. The only time you will need to take action is if you receive a ParentSquare notification that your child has a damaged iPad. You will then receive instructions on how to pay for the $50 deductible for accidental iPad damage so that your child will receive a replacement iPad.
- Families will also be notified if any damage is deemed to be malicious or caused by vandalism.