GREENFIELD PUBLIC SCHOOLS
TECHNOLOGY ACCEPTABLE USE GUIDELINES FOR STAFF
(Revised 09/16/16)

Access to educational technology and its variety of digital resources changes the way we teach, learn, and communicate. For this reason, we have created Technology Acceptable Use Guidelines (AUG) for GPS Employees. In keeping with the District mission, these guidelines encourage the safe use of digital tools and Internet resources in a caring learning environment for all students and staff.

At GPS, computers, electronic services, and other digital resources, (collectively called "technology") exist solely for educational and administrative purposes. Additionally, our technology resources can be used to facilitate communication between and among teachers, administrators, students, staff, and parents/guardians. To this end, all GPS technology use must be consistent with District educational objectives and high priority needs and in compliance with federal, state, and local guidelines for acceptable use. **All documents, resources, messages, and information created, sent, stored, or retrieved on a GPS computer or network are the property of GPS and are subject to monitoring and/or release as a public record.**

A. DEFINITIONS
In this section, we provide definitions of unusual or ambiguous technical terms, words, or phrases that you will encounter in this document.

"**BYOD**" ("Bring Your Own Device") refers to personally-owned wired, wireless, and/or portable digital equipment used for communication, word processing, wireless Internet access, image capture/recording, audio or video recording, and sharing information, etc. Although there is no formal BYOD policy, employees in district buildings with wireless networks are permitted to bring their own devices and connect to the "guest" wireless network for access to educational resources on the Internet. Staff members who access the wireless network with their own digital devices will not be able to view or retrieve any resources stored on District servers.

"**Computer and information technology resources**" ("technology") include, but are not limited to local and wide area wired and wireless networks, Technology Department infrastructure (e.g., servers, firewalls, wiring, switches, wireless access points, backup drives, etc.), Internet access, electronic mail, hardware (e.g., computers, printers, servers, scanners, tablets, interactive whiteboards, digital and document cameras, scientific probes, speakers, monitors, flash drives, etc.), administrative databases, software applications, web-based programs, telephones, and other communications equipment, and related peripherals. [See also "**Technology"** below.]

"**Educational and administrative purposes**" refer to instructional and administrative activities and professional development training of an educational nature.

"Filtering, blocking, and monitoring" refer to the tools the District has in place to restrict access to inappropriate and non-educational websites to ensure compliance with the Children's Internet Protection Act (CIPA), protect important District data, and safeguard network operations.

"**Logging On/Logging Off**" For security purposes, GPS staff members must enter identifier information (i.e., a staff username and password) when "logging on" to a GPS computer. "Logging on" is necessary in order to do computer work. Staff members must "log off" the computer when they are done to prevent unauthorized access by others. In the event a staff member neglects to "log off," the computer initiates an automatic "lock out" after 10 minutes of inactivity. Staff members must then re-enter their staff username and password to return to their work. "Logging off" occurs automatically if a computer shuts down (e.g., due to a power disruption) before a staff member explicitly "logs off."

"**Network**" refers to school and District wired, wireless, and cellular networks accessible to employees.

"**Social Media**" include the various online publications or websites enabling interactive communication or resource sharing over the Internet, i.e., social networks, blogs, websites, Internet forums, and wikis. Social media content can include text, audio, video, images, animations, podcasts, and multimedia communications. websites that facilitate social media include (but are not limited to) Blogger, Edublogs, Facebook, Flickr, Google+, Hi5, Instagram, LinkedIn, Oovoo, Pinterest, Reddit, SchoolTube, Snapchat, Teachers Pay Teachers, TeacherTube, Tumblr, Twitter, YouTube, Vine, WordPress, etc.

"Technology" includes but is not limited to computers, digital resources, electronic services, cellular phones, smartphones, personal digital assistants, MP3 players, USB storage drives, scanners, iOS and Android devices, and portable computers such as laptops, iPads, tablets, Chromebooks, and netbooks. [See also "**Computer and information technology resources**" above.]

"Web Proxy" refers to websites or servers that enable staff members to bypass content filtering. Use of Web Proxies is forbidden in the Greenfield Public Schools.

"**Web 2.0**" refers to Internet tools enabling staff members to produce digital content for viewing or interacting on the Web. Popular examples of Web 2.0 tools include blogs, wikis, classroom websites, and websites used for social networking. The Common Core Standards weave Web 2.0 tools into teaching and learning. For example, Anchor Standard 6 for Writing requires that students "Use technology, including the Internet, to produce and publish writing and to interact and collaborate with others" (http://www.corestandards.org/ELA-Literacy/CCRA/W/6/).

B. GPS TECHNOLOGY AND EMAIL USE

GPS provides a unique staff username and password to all staff members of GPS technology. Employees must use their assigned staff username and password to log on to a GPS computer. The District also provides an email account to every employee. This is the only email service GPS supports and all electronic messaging should be conducted through this email gateway.

1) Each District email user is responsible for the content of the text, audio, or image that (s)he uploads to the Internet or sends through the GPS email system.

2) All GPS email is archived on Google Servers. An employee must preserve all emails and other relevant records related to any incident subject to litigation once that employee is made aware of the legal action.
3) Email messages are considered public records and may be released pursuant to the requirements of the Massachusetts Public Records Act.
4) All communications with GPS parents, guardians, staff, and administrators should be sent through the GPS email gateway.
5) Every email sent from the gpsk12.org domain shall have the following information as part of the signature:

> *Notice: This electronic transmission is only for educational use and must comply with the Acceptable Use Policy of the Greenfield Public Schools. It is for the intended recipient only and may contain information that is privileged, confidential, or otherwise protected from disclosure. Any review, dissemination, or use of this transmission or any of its contents by persons other than the intended recipient is strictly prohibited. If you receive this transmission in error, please notify the sender immediately upon receipt and delete or destroy the communication and its attachments. Under Massachusetts Law, all email created or received by an employee of Greenfield Public Schools is considered a public record and is subject to the requirements of M.G.L. Chapter 66. As a reminder, personally identifiable student data, including name and other information, is protected under confidentiality laws and should only be shared between authorized individuals. Thank you for your cooperation.*

GPS technology and email **should NOT be**:

1) Considered a resource intended for use as a public forum or used for any service not related to GPS business, education or professional development;
2) Used in any way that may harm or tarnish the image, reputation, and/or goodwill of GPS and/or any of its employees; and
3) Used to make any discriminatory, disparaging, defamatory, or harassing comments, or to engage in any conduct prohibited by the GPS Non-Discrimination and Anti-Harassment policy.

C. ACCEPTABLE USE GUIDELINEST FOR TECHNOLOGY AND EMAIL

Several rules govern the acceptable use of GPS technology and email.

1) **ETIQUETTE.** Users of GPS technology and email are expected to abide by the generally accepted rules of network etiquette:
    1. Do not reveal personal information such as last names, addresses, phone numbers, photos, etc. that could identify a staff member or student.
    2. Do not share or reveal passwords
    3. Be polite. Use appropriate, non-abrasive language. Harassment of any kind is prohibited. No message with profane, vulgar, threatening, abusive, defamatory, derogatory, inflammatory, discriminatory, or otherwise objectionable or criminal language remarks about an individual's or a group's race, age,

religion, disability, sex, gender identity, national origin, physical attributes, or sexual preferences will be tolerated or transmitted.

2) You are prohibited from:
    1. Accessing, downloading, posting or transmitting materials that are obscene, sexually explicit, or available from prohibited sites;
    2. Accessing discussion groups or "chat rooms or sending "chain letters," "Non-GPS broadcast" messages, or any other form of online communication whose primary purpose is not educational or GPS-related;
    3. Using GPS technology in a manner that would violate any federal, state, or local law or any GPS policy, including placing information of a non-educational nature on any GPS system, violating copyright, sending threatening material, using Proxy sites to bypass content filtering, spreading computer viruses, Trojans, spam, malware, or any information that would likely result in unexpected work or system downtime and/or the loss of a recipient's work;
    4. Attempting to gain unauthorized access to system programs or computer equipment, including attempts to override or to encourage others to override any network firewalls or filters, or accessing another's home directory, digital desktop, or email without authorization;
    5. Attempting to harm, modify, or destroy another staff member's data;
    6. Discussing highly sensitive or confidential school department information in email communication or sending identifiable confidential student data (such as test scores), or information on other District personnel through email;
    7. Using GPS technology or network resources to gamble, buy, sell, advertise anything not directly related to GPS work/activities;
    8. Using GPS technology or network resources to engage in political campaigning;
    9. Installing software without the written permission of the Director of Technology;
    10. Using an audio recording device, video camera, or camera (or any device with one of these recording devices, e.g. cell phone, laptop, tablet, Chromebook, iPad, webcam, etc.) to record video, capture audio, or take photos on school premises unless you have written permission from the person or persons you are recording;
    11. Participating in other types of use that would cause congestion of the network or interfere with the work of others, (e.g., listening to music streaming from Internet Radio or a service like Pandora or SoundCloud, or watching video from a streaming video service like Netflix, Amazon Prime, etc.); and
    12. Using any information or data whatsoever that would in any way subject the staff member or GPS to any civil or criminal action.

3) **WEB PAGES.** GPS has established a District-wide website that links staff members to Web pages for the District schools. GPS maintains these Web pages for educational purposes, in furtherance of the District's educational mission.
    1. All published pages and corresponding links to any website must relate to GPS's educational mission.

2. GPS teachers who wish to create their own classroom Web pages must have the content of those Web pages approved by their building principal before posting or linking to the GPSK12.org website. Content must conform to all applicable state and federal laws, as well as all District and school committee policies and administrative procedures.
3. Teachers must ensure that all materials on their classroom Web pages comply with the requirements of Section 504 of the Rehabilitation Act and Title II of the Americans with Disabilities Act and are accessible to all students, faculty, staff, and the general public. For example, when including an image, also include a text caption for that image by entering "Alternative Text" in the Image Properties settings for that picture. Additionally, teachers should keep their website information available in more than one format (e.g., print as well as digital) should a visitor to their site experience difficulty with viewing the online content and request access to an alternate format.
4. Website content must not violate copyright or intellectual property laws and the content owner must secure the expressed consent of all involved parties for the right to distribute or publish recordings, photos, images, video, text, slideshow presentations, artwork, or any other materials. Before posting any photographs of students, content owners shall review the list of students whose parents have not consented to having their child's photograph taken or published. No student photograph should be published for personal, promotional use, or any other non-school related purpose.

4) **WEB 2.0.** Before using any Web 2.0 tool with students under the age of 13, employees should review the Privacy Policy and Terms of Use in operation at the tool's website to ensure that usage complies with Children's Online Privacy Protection Act (COPPA) rules designed to protect children under the age of 13 (https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions).

   Additionally, when using Web 2.0 tools either inside or outside the District, employees may NOT:
   1. Harm or tarnish the image, reputation, and/or goodwill of GPS and/or any of its employees;
   2. Attribute personal statements, opinions or beliefs to GPS;
   3. Represent him/herself as an employee or representative of GPS if (s)he is expressing his or her own beliefs and/or opinions;
   4. Use GPS trademarks, logos and any other intellectual property, Greenfield Public School trademarks, logos, and any other GPS intellectual property without prior approval from the building principal or department supervisor; and
   5. Make any discriminatory, disparaging, defamatory, or harassing comments.

D. SOCIAL MEDIA.

Social media can serve as a powerful tool to for learning, communication, and professional development. But educators must give serious thought to the implications of joining an online social network. For example, it is a mistake to assume that what you post online is private. You

should have no expectation of privacy when posting on the Web. Before creating or joining an online social network, ask yourself whether you would be comfortable if a 'friend' decided to send the information to your students, students' parents/guardians, colleagues, or your principal/supervisor.

The following Social Media guidelines identify social media practices for teachers, staff, and other employees in the Greenfield Public Schools.

1) GPS employees should treat professional social media space and communication like a classroom and/or a professional workplace. The same standards expected in GPS professional settings are expected on social media sites. If a particular type of behavior is inappropriate in the classroom or workplace, then that behavior is also inappropriate on the social media site.
2) GPS employees should exercise caution, sound judgment, and common sense when using social media sites.
3) **Authorization:** District presence on any social media site, including school related accounts, such as clubs, teams, field trips, course, or other sites associated with the District or a District school, must be authorized by the staff member's building principal or designee. Any sites, accounts, or pages existing without prior authorization will be subject to review, editing, and removal. As appropriate, a recommendation for disciplinary action may result.
4) **District Logo:** Using GPS District logo(s) on a social media site must receive prior approval from the building principal or department supervisor.
5) **Content Disclaimer:** Any approved official presence on social media sites outside of those created and monitored by the District shall include the following text "The views expressed on this site do not reflect the views of the Greenfield Public Schools (GPS). This site contains user-created content that is not endorsed by GPS. The purpose of this site is (then specify the purpose)."
6) GPS employees are encouraged to maintain a clear distinction between their personal social media use and any District-related social media sites.
7) GPS employees with social media accounts should not post any content that could be considered troubling or inappropriate for school viewing.
8) **Friending District Students**: Employees should not have online interactions with students on social networking sites outside of those approved forums dedicated to academic use. District employees' social networking profiles and personal blogs should not be linked to District students' online profiles. Similarly, District Administrators should not "friend" any GPS employees on their personal social media sites.
9) District employees should use appropriate discretion when using social networks for personal communications and should limit this activity to off-duty hours and the use of their own electronic communication devices.

Although GPS employees enjoy Constitutional rights guaranteed by the First Amendment, certain types of communication, typically by virtue of their subject matter, may have ramifications to the District. Content must conform to all applicable state and federal laws, as well as all District and School Committee policies and administrative procedures.

E. CELL PHONES and BRING YOUR OWN DEVICE (BYOD)

An important District technology goal is to ensure that all employee interactions with technology contribute positively to the learning environment both at school and in the community. Negative use of technology through District-owned devices inside or outside our schools is unacceptable. The use of technology whether owned by the District or supplied by staff members entails personal responsibility. Employees shall comply with District rules, act in a responsible manner, and honor District terms and conditions. Failure to comply with such terms and conditions may result in temporary or permanent loss of access as well as other disciplinary or legal action as necessary.

Use of personal technology/devices may violate the District's Acceptable Use Policy for Students if the District reasonably believes the conduct or speech will cause material disruption of school activities or an employee's ability to perform his or her job duties. Therefore, employees may use their personal electronic devices at work only with the express permission of their building principal or the Superintendent of Schools. If permission is granted, all guidelines, procedures, and rules for Acceptable Use outlined in this document would apply.

1. The employee acknowledges that school and District network filters will be applied to Internet access and understands that no attempt may be made to bypass them. Only the school or District Internet gateway may be accessed while on campus. Personal electronic devices with Internet capabilities (such as cell phones, cell network adapters, mobile hot spots, etc.) should not be used to access the Internet at any time, without the express prior permission of the building principal or department supervisor.
2. Cell phones must be in silent mode while the employee is in District. A teacher's cell phone must not be visible on the teacher's desk during the school day. It should be stored in a secure location, i.e. in a vehicle, pocket, purse, locker, backpack, etc.
3. A personal cell phone (or other Personal Electronic Device) may be used without any limitation, during breaks or lunchtime, unless it overly distracts or interrupts other students, teachers, parents, faculty members, or employees. Teachers may not use their cell phones or personal electronic devices when class is in session without express permission from the building principal and only for school-related uses.
4. Responsibility for the personal electronic device rests with the individual owner. GPS is not liable for any device stolen or damaged on campus.
5. The employee understands that bringing on premises or infecting the network with a Virus, Trojan, malware, or program designed to damage, alter, destroy, or provide access to unauthorized data or information is in violation of the AUG policy and will result in disciplinary action.
6. GPS has the right to collect and examine any device suspected of causing problems or virus/malware infections.

F. FILTERING

While GPS buildings utilize Internet "filtering, blocking, and monitoring" tools to restrict access to inappropriate and non-educational websites, it is impossible to control access to all Internet materials. There is no absolute guarantee that a teacher may not discover inappropriate content. You are cautioned that many of these pages include offensive, sexually explicit, and inappropriate content. In addition, having an email address may lead to the receipt of unsolicited

email containing offensive content. You access the Internet at your own risk. GPS is not responsible for Internet material viewed or downloaded by its staff members.

If a staff member finds materials that are inappropriate while using GPS technology, (s)he will:

1. Refrain from downloading, identifying or sharing the material; and
2. Report his/her discovery of such materials to the building.

G. PIRACY

Information and media piracy is a federal offense that is punishable by a fine or imprisonment. GPS prohibits illegal distribution (otherwise known as pirating) of text, software, movies, songs, or other copyrighted materials.

H. LIMITED PERSONAL USE

GPS does not grant ownership or copyright to the contents of any message posted on GPS resources or equipment, e.g., email, lesson plans, et al. Any posting on GPS resources remains the property of the District.

Personal use is prohibited if:

1. It interferes with the use of District technology resources;
2. Such use burdens the District with additional costs;
3. Such use interferes with the staff member's employment duties or other obligations to the District; or
4. Such use includes any activity that is prohibited under any GPS District rule (including this rule), School Committee policy, or state or federal law.

I. LEGAL REQUIREMENTS

GPS is committed to complying with applicable information security requirements and relevant information security standards and protocols. These requirements include, but are not limited to, the following:

1. The Family Educational Rights and Privacy Act (FERPA);
2. Children's Internet Protection Act (CIPA);
3. Individuals with Disabilities Education Act (IDEA);
4. Children's Online Privacy Protection Act (COPPA);
5. Protecting Children in the 21st Century Act;
6. Health Insurance Portability and Accountability Act (HIPPA);
7. Section 504 of Rehabilitation Act; and
8. Americans with Disability Act (ADA)

Employees who use GPS network and technology resources are required to adhere to state and federal law as well as GPS School Committee policy. Any attempt to break those laws or policies through the use of GPS networks, technology, and email or through personal electronic devices may result in discipline or litigation against the offender(s) by the proper authorities. GPS will provide any information necessary in order to cooperate fully with the appropriate authorities in the civil and/or criminal process.

J. NO EXPECTATION OF PRIVACY

In accordance with FERPA, CIPA, IDEA, COPPA, the Protecting Children in the 21st Century Act, and HIPPA, individuals should not have an expectation of privacy when using GPS email, systems, or equipment.

GPS stores copies of all information created on or sent from District-owned digital devices. By utilizing the school's technology and email services, staff members indicate their acknowledgement that digital documents, images, and other files along with electronic mail messages are not considered confidential and consent to monitoring and access.

Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of criminal activity to law enforcement.

Under the Massachusetts Public Records Law, electronic mail transmissions and other uses of electronic resources by GPS employees may be considered public records. While GPS does not plan to review stored or back-up files on a regular basis, it reserves the right to access them as necessary in the ordinary course of its business, for purposes including, but not limited to, ensuring proper use of resources and conducting routine network maintenance.

Communications, text, audio, video, and images may be disclosed to administrators, law enforcement in response to legal requests, or other third parties in the context of legal requests in the course of litigation without prior consent of the sender or receiver or pursuant to other legal requirements, including but not limited to public records requests or informational requests under M.G.L. Ch. 150E.

School administrators and their authorized employees may, for a legitimate reason, perform the following:

1. Obtain emails sent or received on District email.
2. Confiscate and/or search District-owned software or equipment.

(Page left intentionally blank)

K. SIGNATURE

I understand and will abide by the above Acceptable Use Guidelines. I further understand that any violation of the Acceptable Use Guidelines may result in suspension or termination of access privileges and may result in disciplinary action up to and including termination consistent with the disciplinary policies of the Greenfield Public Schools and the applicable provisions of any governing collective bargaining agreement. If a violation of these guidelines may constitute a crime, then that violation also mays be reported to the proper authorities and may result in criminal prosecution.

_____ _____

Signature of Employee **Printed Name**

Date: _____ **Building Location: _____**

(

(Page left intentionally blank)

s

SOCIAL MEDIA SITE AUTHORIZATION FORM

Employees of the Greenfield Public Schools who wish to create and maintain an official District or school presence on any social media site must have a copy of this completed form on file in the school Principal's office or the Department Supervisor's office, **prior** to a social media site's activation. Either a hard copy or .pdf copy filed electronically is acceptable. Once authorized by a school principal/department supervisor and superintendent, the author is fully responsible for regularly maintaining the site, appropriate online conduct, and adhering to the District's official Social Media Guidelines described in the Technology Acceptable Use Guidelines for Employees of the Greenfield Public Schools.

Date: _____ Dept. or School Site: _____

Employee Name: _____ ID: _____

Employee Title: _____ District email: _____

Nature of request:

- □ Website/page: _____
- □ Blog: _____
- □ Other: _____
- □ Other: _____
- □ Other: _____

Purpose of presence on social media site:

SITE ACCOUNT INFORMATION:

E-mail address associated with site: _____

Username: _____ Password: _____

AUTHORIZATION BY SCHOOL PRINCIPAL AND SUPERINTENDENT:

Name: _____ Signature: _____

Title: _____ Date: _____

Principal/Dept. Supervisor: _____ Superintendent: _____

Carol S. Holzberg, PhD, CETL, Director of Technology
September 16, 2016