TAUNTON PUBLIC SCHOOLS
Internet Acceptable Use and Social Networking Policies and Administrative Procedures

A. INTERNET ACCEPTABLE USE POLICY OF THE TAUNTON PUBLIC SCHOOLS

I. Mission Statement:

Academic excellence for every student, in every classroom, in every school.

II. Purpose:

The Taunton Public School District shall provide access for employees and students to the computer network, including access to external networks, for purposes of advancing the interest and educational purposes of the Taunton Public Schools. Educational purposes shall be defined as classroom activities, career and professional development, and self-discovery activities of an educational nature. The purpose of the computer network is to assist in preparing students for success in life and work by providing access to a wide range of information and the ability to communicate with others. The computer network will be used to increase communication (staff, parent and student), enhance productivity, and assist staff in upgrading existing skills and acquiring new skills through a broader exchange of information. The computer network will also be used to provide information to the community including parents, governmental agencies, and businesses.

III. Acceptable Use:

The Superintendent or designee shall implement the Internet Acceptable Use Policy, the Social Networking Policy for Staff and their associated Administrative Procedures, and all user agreements, consistent with the purposes and mission of Taunton Public School District as well as with applicable federal and state law and governing collective bargaining agreements.

IV Availability:

The Superintendent or designee shall implement, monitor, and evaluate the district's computer network for instructional and administrative purposes as provided herein.

Access to the computer network, including external networks, shall be available to employees and students for instructional and administrative purposes and in accordance with the Internet Acceptable Use Policy, the Social Networking Policy for Staff and their associated Administrative Procedures.

All users shall be required to acknowledge receipt of this policy, the Social Networking Policy (staff only) and their associated Administrative Procedures, which together govern the use of electronic media by students and employees of the District and shall agree in writing to comply with these policies and administrative procedures. Noncompliance with the Internet Acceptable Use Policy, the Social Networking Policy for Staff and their associated Administrative Procedures may result in suspension or termination of certain user privileges and other disciplinary actions, including the possibility of suspension or expulsion for students, and suspension or dismissal for employees subject to the applicable provisions of any governing collective bargaining agreement and consistent

with the policies of the Taunton Public Schools and relevant law(s). Violations of law may result in criminal prosecution as well as disciplinary action by the Taunton Public Schools subject to the applicable provisions of any governing collective bargaining agreement and relevant law(s).

V Monitored Use:

Electronic mail transmissions and other use of electronic resources by students and employees utilizing the District's electronic mail accounts shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use for instructional and administrative purposes. Copies of all information created, sent or retrieved are stored in the District's backup files. The District reserves the right to access and monitor all messages and files on the District's computer system as it deems appropriate in the ordinary course of its business, including, but not limited to ensuring proper use of resources and conducting routine maintenance. . Where appropriate, communications, including text and images, may be disclosed to law enforcement officials without prior consent of the sender and receiver.

VI Liability:

Except as otherwise provided in an applicable collective bargaining agreement, Massachusetts General Laws, or this policy, the Taunton Public Schools shall not be liable for users' inappropriate use of electronic resources or violations of copyrighted or restricted material, or for costs incurred by users which are knowingly not related to acceptable use under this policy. The Taunton Public Schools shall not be responsible for ensuring the accuracy or usability of any information found on external references.

By signing the "Staff Internet Use Agreement" form the employee accepts responsibility for his/her own actions in using the District's computer system. By signing the "Student Internet Use Agreement" form the student accepts responsibility for his/her own actions in using the District's computer system.

VI1 Acknowledgment:

Each user will sign the appropriate Student or Staff Internet Use Agreement form (Attachments A and B) before receiving access to the District's computer network. Parent/Guardians must also sign for student access.

B. <u>SOCIAL NETWORKING POLICY FOR STAFF</u>

I. Internet Acceptable Use Policy Still In Force

This policy is adopted in addition to, and not as a substitute for, the School District's Internet Acceptable Use Policy, which governs use of the school district's technological resources for students and staff.

II. Purpose

The Taunton Public Schools recognizes the proliferation and, in some instances, usefulness, of online conversation between educators and students and/or their parents or guardians. However, due to the nature of social networking sites, there exists a risk, without proper care and planning, that the lines between one's

personal and professional life may be blurred. Employees should always be mindful of how they present themselves to the world, online and otherwise. Should an employee make the decision to "friend" a student on Facebook, subscribe to a student's "twitter" account, regularly engage in email "chat" with a student, exchange in text messages with students or engage in other electronic communication, such activities may compromise healthy student and staff boundaries.

Online communication using one's own personal resources, as opposed to school district resources, also compromises the educator's and District's, ability to retain public records in accordance with the requirements of the Commonwealth's public records laws. Public employees who send, receive or maintain records in their capacity as public employees, must retain, disclose and dispose of such records in compliance with the strict provisions of the public records law. This law applies to all forms of records, including paper and electronic communication. When employees communicate through school-based resources, records are retained and archived through the District's technology department. If, however, non-District resources are used, such information is not able to be retained by the District. The legal requirement of retention does not change if personal sources are used. Therefore, the burden falls on the employee to comply with public records laws when using personal email or social network accounts to communicate with students and/or parents and guardians. Failure to so comply may result in disciplinary action.

III. Expectations

Taunton Public Schools adopts the following expectations for the use of electronic media for all staff members:

1. The best way to eliminate risks associated with a staff member's use of personal social media with students is to avoid it.

2. Should a staff member determine that there is a meaningful, educational purpose for engaging in the use of social media with students, s/he shall take responsibility for any information that is posted on any social networking site they utilize. Staff members should not post anything they would not want their immediate supervisor or their Superintendent to read.

3. When engaging in electronic communication, staff members should apply the same principles used in other forms of communication, including the use of discretion and an awareness of the possibility that the communication may be shared with others. Staff members are reminded that by hitting "send," they effectively eliminate their ability to control to whom the message will be forwarded in the future.

4. Staff members shall adhere to appropriate staff/student boundaries in all communications, electronic or otherwise.

5. Staff members shall adhere to student privacy rights, student record laws and the laws and rights of employees and students to have their personnel and medical information kept confidential at all times. Information that is protected by law from disclosure to third parties will not be communicated online in a way that subjects such information to retrieval by those third parties.

6. Staff members should communicate electronically with students and parents on educational matters only, and only through District-based electronic resources or District approved social networking accounts. Use of personal email account, personal cellular phones, or personal social networking accounts to discuss school business with students and parents is strongly discouraged and should only be allowed if no other District-based electronic resources can be used for the communication. Information sent or received by educators or Taunton Public School staff members through

personal email, personal cellular phones or personal social network accounts related to the individual's employment in the Taunton Public Schools are subject to public records retention, exemption and disclosure requirements, and may be reviewed and examined by the District at any time.

7. The District recognizes that, in limited cases, use of cell phone text messages or cell phone calls or emails outside of regular school hours may be useful. For example, in connection with school sponsored events for which staff members serve as duly appointed advisors, they may need to convey messages in a timely manner to students and may not have access to school based email accounts, school provided telephones or school based web pages. In such limited circumstances, staff member shall copy their direct supervisor or immediately forward the on the electronic communication to them.

8. Any conduct or communication, whether online or not, that is inappropriate, unprofessional, undermines a staff member's ability to instruct or maintain control and discipline with students, compromises one's objectivity, or harms students, is considered to be a violation of this Policy. A staff member may also face individual liability for inappropriate online communications with students and/or parents and guardians.

9. There is no expectation of privacy for staff members who use personal email or other electronic media accounts when accessed using school district technology

10. Staff members shall maintain professionalism in all electronic communications.

11. When using Facebook or other social networking accounts, a staff member may not, without express permission from the Superintendent of Schools, use or post the school's or District's logo, likeness or any school photographs or other property that belongs to the District. Additionally, no staff member may use or post any photographs of a student or students (or list the name or names of students) without express written consent of the student and/or their parent or guardian (if the student is under 18 years old).

12. Staff members should immediately report any inappropriate messages they receive from a student, parent, colleague, or another staff member to their immediate supervisor(s) or building principal.

IV. Miscellaneous

1. This policy is not intended to infringe upon a staff member's right to speak publicly on matters of public concern or to communicate with fellow members of their union on workplace issues so long as such communication adheres to appropriate time, place and manner restrictions, complies with the provisions of this policy, the Internet Acceptable Use Policy, and the associated Administrative Procedures and does not interfere with the performance of any job duties.

2. References to "Facebook" are not included to limit application of this policy to the sole use of that program. All online, electronic or computerized means of communication are subject to this policy. Given the rapid pace of technological change it is impossible to identify all proprietary or commonly named or identified means of such communications.

C. ADMINISTRATIVE PROCEDURES GOVERNING THE INTERNET ACCEPTABLE USE POLICY FOR STAFF AND STUDENTS AND THE SOCIAL NETWORKINGPOLICY FOR STAFF

1. The District will provide each user with one copy of the District's Internet Acceptable Use Policy, the Social Networking Policy (staff only) and these Administrative Procedures. Access to the District's computer network will be granted to a user only after he/she signs the appropriate Internet Use Agreement Form and returns it to his/her building principal who will then forwarda copy to the Personnel Office to be placed in his/her personnel file.

2. Employees should not permit students to use the District's computer network if they have not signed the Acceptable Internet Use Policy and do not appear on the roster of approved computer users who have access to the District's computer network. Access will only be granted to students with a signed Internet Use Policy and permission of building administrator or designee(s).

3. Passwords are confidential. All passwords shall be protected by the user and neither shared, nor displayed.

4. Principals or their designee will be responsible for disseminating these policies and procedures in the building(s) under their control. Principals or their designee will ensure that all users complete and sign an agreement to abide by policies and procedures regarding use of the computer network.

5. Individual users shall, at all times, be responsible for their use of accounts issued in their name.

6. A student record is kept by the public school and includes any information concerning a student that is organized on the basis of the student's name or in such a way that a student may be individually identified l. This includes any documents and communication generated using all types of electronic media and all parts (i.e. subject line, body) of electronic communication. Any electronic communication should be written with the awareness that it may be shared with a parent, a member of the general public (e.g. newspaper) or the Superintendent of Schools.

7. The District's Technology Department shall be responsible for establishing appropriate retention and backup schedules. Before any information is deleted from the District's computer network by anyone using the system, employees should ensure that it is permissible to delete pursuant to all applicable federal and state public, health and student records laws.

8. Taunton Public Schools shall be authorized to monitor or examine all system activities of all users including electronic mail transmissions, as deemed appropriate to ensure proper use of electronic mail resources.

9. System users should only purge electronic information according to District retention guidelines, which shall occur consistent with all applicable federal and state public, health, and student records laws.

10. System users may redistribute copyrighted material only with written permission of the copyright holder or designee. Such permission must be specified in the document or in accordance with applicable copyright laws, the District's Internet Acceptable Use Policy, the Social Networking Policy for Staff and these Administrative Procedures. Copyrighted software or data shall not be distributed or placed on the district computer network without permission from the holder of the copyright and the system administrator.

11. System administrators may upload/download public domain programs to the computer network. System administrators are responsible for determining if a program is in the public domain.

12. Commercial use of the computer network is prohibited.

13. A system user's account may be deactivated/disabled after 30 days of non-use, unless such non-use is due to an approved leave of absence for the user.

14. The District's computer network may not be used for illegal purposes, in support of illegal activities, for any activity prohibited by District policy, or in any way that would constitute conduct unbecoming a school department employee.

15. System users shall not use another user's account without the user's permission.

16. Any malicious attempt to harm, improperly access, or destroy equipment, material data, or programs is prohibited.

17. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of District policy and/or as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creation of computer viruses.

18. Vandalism will result in the cancellation of system privileges and will require restitution for costs associated with hardware, software, and system restoration, and will result in disciplinary action.

19. Forgery or attempted forgery is prohibited.

20. Attempts to read, delete, copy or modify the electronic mail of other users or to interfere with the ability of other users to send/receive electronic mail is prohibited.

21. Users should always use appropriate language; swearing, vulgarity, ethnic or racial slurs and other inflammatory language is prohibited and may result in disciplinary action.

22. Pretending to be someone else when sending/receiving messages is prohibited.

23. Transmitting or viewing obscene or vulgar material, i.e. material deemed harmful to minors under the Children's Internet Protection Act, is prohibited.

24. Revealing personal information without the person's permission (name, address, phone numbers, photograph, etc.) is prohibited.

25. The District will cooperate fully with local, state, or federal officials in any investigation concerning or related to alleged misuse of the district's computer network.

26. Principals or their designee will support employees in the enforcement of the District's Internet Acceptable Use Policy, the Social Networking Policy for Staff and these Administrative Procedures

27. Computer Viruses: Though all of our computers have virus-scanning software, the data files are not always up-to-date especially with respect to new viruses. Most viruses are transmitted by CDs, USB drives, e-mail and Internet downloads. If a staff member suspects a virus on his/her computer, he/she is asked to call the Director of Technology immediately. If an employee works on a home computer and uses e-mail or USB drives/CDs to transmit files, the employee should make certain the home computer has up-to-date virus scanning software.

28. A user who knowingly violates the District's Internet Acceptable Use Policy, the Social Networking Policy for Staff and these Administrative Procedures will be subject to suspension or termination of computer network privileges and may be subject to appropriate disciplinary action, including the possibility of suspension or expulsion (in the case of a student), or suspension, dismissal, and/or prosecution (in the case of an employee), in accordance with the applicable provisions of any governing collective bargaining agreement and other applicable federal and state laws.

Common Sense Rules for the Use of Electronic Media

- Be polite. Do not send abusive messages/postings to others.
- Use appropriate language. Offensive, bullying, obscene, vulgar, defamatory, threatening, discriminating, harassing, or inflammatory language will not be tolerated in any public or private message.
- Adhere to copyright and licensing agreements.
- Do not deliberately or inadvertently spread computer viruses.
- Do not use/view another person's files/drives (Z: Drive, J: Drive, etc) without permission.
- Do not destroy, abuse, modify, or improperly access the school's hardware or software.
- Do not illegally distribute software.
- Do not place unlawful information into electronic media.
- Do not use electronic media for commercial purposes, product advertising, or political lobbying.
- Do not access, download, store, or print files that are offensive, bullying, obscene, vulgar, defamatory, threatening, discriminating, harassing, or inflammatory.
- Do not post another person's personal information such as home phone number, address, or photographs. Take precautions when posting personal information about yourself.
- Keep your password private and keep in mind that it is wise to frequently change passwords.
- Do not interfere with, harm or modify the work of other users.
- Staff members should treat all electronic communications as a public record, or something you would print and put into a student record file or share with a parent, a member of the general public (e.g. newspaper) or the Superintendent of Schools.
- Student users should never discuss highly sensitive or confidential information in e-mail communications.
- Student/staff relationships and parent/staff relationships via electronic media sources (including email, Facebook, Twitter, text messages, or the like) should be limited to necessary school-related issues only.
- Email (using personal or work email accounts) sent during the work day or at anytime if work related, is a public record and/or a student record.
- It is impossible to guarantee the confidentiality and security of any transmission made on the Internet.

Attachment "A"
TAUNTON PUBLIC SCHOOLS
Taunton, Massachusetts

STUDENT INTERNET USE AGREEMENT

Student User Name: _____

School: _____

Grade: _____

I/We acknowledge that we have been given the opportunity to review the District's Internet Acceptable Use Policy, and the associated Administrative Procedures a copy of which can be found on the Taunton Public Schools website at www.tauntonschools.org*. I/We understand, and will abide by the Taunton Public School's Internet Acceptable Use Policy, and the associated Administrative Procedures. I/We understand the terms and conditions of use of the District's computer network. I/We further understand that any violation of the District's Internet Acceptable Use Policy, and the associated Administrative Procedures shall be considered unethical and may constitute a criminal offense. I/We recognize that should any violation be committed, access privileges may be revoked and school disciplinary actions and/or legal action may be taken.

_____ _____
Student's Name **Student's Signature**

_____
Date

_____ _____
Parent/ Guardian's Name **Parent/Guardian's Signature**

_____
Date

* I understand that I can contact my building principal to obtain a hard copy of the Taunton Public School's Internet Acceptable Use Policy, and the Associated Administrative Procedures if needed.

Attachment "B"
TAUNTON PUBLIC SCHOOLS
Taunton, Massachusetts

STAFF INTERNET USE AGREEMENT

Please Print

Employee's Name: _____

School: _____

Position: _____

This is to certify that I have been provided with a copy of the District's Internet Acceptable Use Policy, the Social Networking Policy for Staff and the associated Administrative Procedures approved by the Taunton Public School District's School Committee. I understand and will abide by the District's Internet Acceptable Use Policy, the Social Networking Policy for Staff and the associated Administrative Procedures. I understand the terms and conditions of my use. I further understand that any violation of District's Internet Acceptable Use Policy, the Social Networking Policy for Staff and the associated Administrative Procedures may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and school disciplinary actions and/or legal action may be taken.

Signature: _____ **Date:** _____