# Employee Appropriate Use Policy of Information Technology Resources – Regulations

**Appropriate Uses:** The Weston Public Schools ("WPS") information technology ("IT") resources shall be used in a manner consistent with the educational mission as well as providing citizens with better and more efficient services. The user shall show respect of the shared resource, software, intellectual property rights, ownership of information and system security. Professional behavior and means of communication are expected. Use contrary to this policy or rules is unacceptable and prohibited.

**Prohibited Uses:** Each WPS employee is responsible for his/her actions involving information technology and his/her computer files, passwords and accounts. Examples of prohibited use of school IT include, but are not limited to, the following:

1. Any use that violates any federal, state or local law or regulation, including copyright laws, or violates a School Committee policy;
2. Any use to harass, discriminate, threaten, defame, demean or intimidate;
3. Any use that involves material or language that is profane, obscene, fraudulent, offensive, sexually explicit or sexually suggestive, or vulgar;
4. Any use for private financial gain, advertising, or solicitation purposes;
5. Conducting private business;
6. Fundraising for any non-school sponsored purpose, whether non-profit or for-profit;
7. Downloading, using or copying software in violation of a license agreement or copyright;
8. Infringing on intellectual property rights;
9. Connecting any device not owned and managed by the WPS to the network (other than the "Open" wireless network);
10. Obtaining confidential information about student and/or their families for non-school related activities or sharing confidential information about students or WPS employees for non-school related activities;
11. Wasteful use of the schools IT resources by, among other things, sending mass mailings or chain letters, excessive printing, spending excessive amounts of time on the Internet, or otherwise creating unnecessary network traffic. For the purposes of this section "excessive amounts of time" is time that interferes with the employee's official duties and responsibilities;
12. Revealing one's password to anyone else, using another's password, or pretending to be someone else when sending information over the school network;
13. Forgery or attempted forgery;
14. Gaining or attempting to gain unauthorized access to any computer or network;
15. Any misuse or disruption of school IT, including intentional physical misuse or damage, or any breach or attempt to breach the security features of school IT;
16. Any communication that represents personal views as those of the schools or that could be misinterpreted as such;
17. Any communication that violates generally accepted rules of electronic mail or computer etiquette and/or professional conduct;

18. Posting pictures, audio, or video of school personnel, students, or school related activities to the Internet without the permission of administration, faculty, and the parents of all students involved; and
19. Failure to report a breach of school IT security to the Director of Information Technology and School Libraries.

WPS employees who need further clarification or have a question should seek guidance from their building Principal and/or the Director of Information Technology and School Libraries.

**Privacy:** The use of school IT resources varies greatly from personal home use. All actions including, but not limited to, information stored, accessed, viewed or written are logged and accessible by the Administration. The WPS has the right to monitor, quarantine, backup, move, archive and/or delete, and access all electronic files, local or remote, on systems managed by the district. WPS employees should have no expectation or guarantee of privacy when using the school's IT resources whether their use takes place during or outside working hours.

All actions performed by WPS employees in regards to the schools' IT resources are legally discoverable and could be subpoenaed by a court of law.

**Data Confidentiality:** Some WPS employees, as part of their jobs, have access to confidential information such as personal data about identifiable individuals. WPS employees are expected to use appropriate judgement and caution in communications concerning students and staff to ensure personally identifiable information remains confidential. WPS employees are strictly prohibited from acquiring access to and/or disseminating such confidential information unless access to and/or dissemination is authorized and required by their jobs.

Resources, such as websites, blogs, wikis, assessments, etc., used or created as part of an employee's responsibilities with the WPS should be known by and assessable by the appropriate administrator (Department Head, Director, Principal, or other District Administrator) and pre-approved by the Director of IT for continuity, safety, and liability. Resources provided by the WPS are always preferred to external options unless none are available.

**Email and the Public Records Law:** Email messages concerning official school business are generally considered public record information that is subject to disclosure under the Massachusetts public records law. [G.L. c. 66 section 10; G.L. c. 4, s. 7 (26)]

Documents prepared in anticipation of litigation or to reply to a Freedom of Information Act (FOIA) should not be disclosed without prior approval from the Superintendent.

**Etiquette:** Use of all communications (electronic or written) reflect upon the Town of Weston and Weston Public Schools. WPS employees should communicate in a professional manner with proper spelling and grammar. Modeling for students is expected of all staff in and outside of the classroom. Be mindful of your use of social media (Facebook, My Space, etc.) as parents, students, and community members, rightfully or not, may conduct their own search of you. Such searches may

result in discovery of personal postings and/or and your comments made about work, fellow faculty/staff, and/or students. Therefore, WPS employees are held to a higher standard of conduct that reflects on your reputation and that of WPS.

Supervisors may, in their discretion, require that work-related e-mail messages be approved as to form and content prior to dissemination.

**Responsibility for Laptops Issued to Faculty and Staff:** An employee who has been issued a laptop is responsible for the laptop at all times in school and outside of school. There should be no expectation that stolen or damaged laptops will be replaced with similar equipment. Negligent or excessive damage to WPS equipment may result in repair/replacement charges. Only software with appropriate licenses owned by WPS can be installed on the laptop.

**Responsibility for Unauthorized Charges, Costs or Illegal Uses:** WPS assumes no responsibility for any unauthorized charges made by WPS employees, including but not limited to credit card purchases, subscriptions, long distance telephone charges, equipment and line costs, or for any illegal use of its computers, such as copyright violations.

**Disclaimer on Liability:** WPS assumes no responsibility for any loss or corruption of data resulting from the use of the schools IT resources.

**Violation of the Policy:** Violation of any portion of this policy may result in disciplinary and/or legal action, and/or including possible suspension or dismissal.