


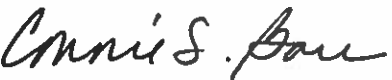
Policy for: STAFF RESPONSIBLE USE OF DIGITAL RESOURCES		Revision
Date Approved by School Committee: July 7, 2015	Signature of Chair  Connie S. Barr	Page 1 of 7

Technology Resources Purpose:

Access to network resources, electronic communications, the Internet, database systems, computers and other information technology (IT) resources is essential to the mission of the Needham Public Schools (NPS). The purpose of these resources is primarily to develop, deliver, and support quality educational materials in the pursuit of excellence in teaching and learning and to efficiently manage the day-to-day operations of the NPS.

Information Technology will be used in a manner consistent with the educational mission of the Needham Public Schools. The user will exercise good and professional judgment in the use of shared resources, software, intellectual property rights, ownership of information and system security. Professional behavior and communication are expected at all times. All home use of NPS computers and district-provided accounts and resources must adhere to the terms and conditions of acceptable use as outlined in this policy. Use contrary to this policy (IJNDB-1) is unacceptable and prohibited.

Use of any of the schools' IT resources by any user will constitute acceptance of the terms of this policy and of any further amendments. All staff will sign an acknowledgment that they have read the Staff Responsible Use policy. A failure to comply with the acknowledgement provision does not relieve a user of the obligations and responsibilities of the Responsible Use Policy.

Policy for: STAFF RESPONSIBLE USE OF DIGITAL RESOURCES		Revision
Date Approved by School Committee: July 7, 2015	Signature of Chair  Connie S. Barr	Page 2 of 7

Privacy:

Employees should have no expectation or guarantee of privacy when using the schools' IT resources whether their use takes place during or outside working hours. All actions including, but not limited to, information stored, accessed, viewed or written are logged and accessible by the Administration. The NPS 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.

All actions performed by employees in regards to the schools' IT resources are legally discoverable and could be subpoenaed by a court of law and are potentially considered to be public records under Massachusetts and federal statute.

Data Confidentiality:

Some employees, as part of their jobs, have access to confidential information such as personal data about identifiable individuals. Personally identifiable information remains confidential; employees are expected to use appropriate judgment and caution in communications concerning students and staff. 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. Digital information may be subject to federal (FERPA) and state privacy statutes.

Employees are expected to exercise reasonable judgment in the use of private student data and only as part of their employment responsibilities with the Needham Public Schools. This includes the use of electronic student data that may be transported on devices, computers, drives, and in other ways to

Policy for: STAFF RESPONSIBLE USE OF DIGITAL RESOURCES		Revision
Date Approved by School Committee: July 7, 2015	Signature of Chair <i>Connie S. Barr</i> Connie S. Barr	Page 3 of 7

and from the workplace. If an employee suspects or believes private student data and records have been lost, stolen, or otherwise compromised, the employee should immediately notify her/his supervisor.

Curriculum and Resources:

Resources used to create websites, blogs, wikis, assessments, or other communications and learning experiences as part of an employee's responsibilities with the NPS may be pre-approved and accessible by the appropriate administrator (Department Head, Director, Principal, or other District Administrator) to ensure program consistency, continuity, safety, and liability. Employees must adhere to appropriate copyright laws and guidelines when developing, using, and/or reproducing protected material.

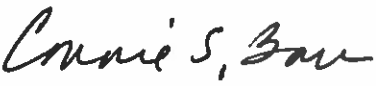
Email and the Public Records Law:

Email messages concerning official school business are generally considered public record information that is subject to disclosure under the Massachusetts Public Records Law. (M.G.L. Chapter. 66 Section 10: M.G.L., Chapter 4, Section 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.

Professional Communication and Practices:

Employees should communicate in a professional manner. Communication between and among staff, students, and families should be educationally relevant, including the use of social media.

Policy for: STAFF RESPONSIBLE USE OF DIGITAL RESOURCES		Revision
Date Approved by School Committee: July 7, 2015	Signature of Chair  Connie S. Barr	Page 4 of 7

Supervisors may choose to approve the form and content of work-related communication prior to dissemination.

Prohibited Uses:

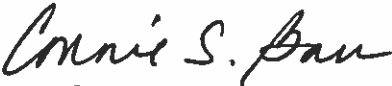
Each employee is responsible for his/her actions involving information technology and his/her computer files, passwords and accounts. Examples of prohibited use of school IT include, but are not limited to, the following:

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 vulgar, profane, obscene, fraudulent, offensive, sexually explicit or sexually suggestive;
4. Any use for private financial gain, advertising, online gambling or solicitation purposes;
5. Conducting private business that is not incidental in nature;
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 NPS to the internal school network (other than the "Open" wireless access to the Internet) without permission from the technology administrator;
10. Obtaining confidential information about students and/or their families for non-school related activities or sharing confidential

SCHOOL COMMITTEE POLICY
NEEDHAM PUBLIC SCHOOLS

FILE


IJNDB -1

Policy for: STAFF RESPONSIBLE USE OF DIGITAL RESOURCES	Revision
Date Approved by School Committee: July 7, 2015	Signature of Chair  Connie S. Barr

Page 5 of 7

- information about students or employees for non-school related activities;
11. Sending mass electronic mailings or chain letters, excessive printing, spending excessive amounts of time on the Internet that interferes with the employee's official duties and responsibilities; or otherwise creating unnecessary network traffic;
 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 [i.e. hacking];
 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 interpreted as such;
 17. Any communication that violates generally accepted rules of electronic mail or computer etiquette and/or professional conduct;
 18. Posting pictures or audio, or identifiable information of students, administration, faculty, and the parents of students that is not educationally relevant;
 19. Failure to report a breach of school IT security to the employee's supervisor;
 20. Using District resources for union business that is not incidental in nature;
 21. Any other misuse identified by District administration.

Employees who have a question or need further clarification about these prohibitions should seek guidance from their building principal or supervisor.

Policy for: STAFF RESPONSIBLE USE OF DIGITAL RESOURCES		Revision
Date Approved by School Committee: July 7, 2015	Signature of Chair  Connie S. Barr	Page 6 of 7

Responsibility for Laptops/Mobile Devices Issued to Faculty and Staff:

An employee who has been issued a laptop or other mobile device is responsible for the equipment at all times in school and outside of school. Upon the conclusion of an individual's employment with the Needham Public Schools, the employee will return all school issued technology and technology devices.

Responsibility for Unauthorized Charges, Costs or Illegal Uses:

NPS assumes no responsibility for any unauthorized charges made by 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:


NPS makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through its network will be error-free or without defect. The District will not be responsible for any damages users may suffer, including but not limited to, loss of data or interruptions of service, or personal, physical, psychological, or monetary damages. Users are responsible for backing up their own data. The District will not be responsible for unauthorized financial obligations arising through the employee use of digital resources.

This policy is not all-inclusive. NPS reserves the right to notify an employee of any other impermissible action regarding the use of the computer or

SCHOOL COMMITTEE POLICY
NEEDHAM PUBLIC SCHOOLS

FILE

IJNDB -1

Policy for: STAFF RESPONSIBLE USE OF DIGITAL RESOURCES		Revision
Date Approved by School Committee: July 7, 2015	Signature of Chair  Connie S. Barr	Page 7 of 7

Internet. Due to the rapid evolution of technology this policy will need periodic review.

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.

References:

Children's Internet Protection Act (CIPA)
Title XIV: Child Online Protection Act (COPA)
Family Educational Rights and Privacy Act (FERPA)