

1 **Nashua School District**

2
3 **STUDENTS**

3612P
page 1 of 5

4
5 Acceptable Use of Electronic Networks

6
7 All use of electronic networks shall be consistent with the District’s goal of promoting
8 educational excellence by facilitating resource sharing, innovation, and communication. These
9 procedures do not attempt to state all required or proscribed behaviors by users. However, some
10 specific examples are provided. **The failure of any user to follow these procedures will result**
11 **in the loss of privileges, disciplinary action, and/or appropriate legal action.**

12
13 Terms and Conditions

- 14
15 1. Acceptable Use – Access to the District’s electronic networks must be: (a) for the purpose of
16 education or research and consistent with the educational objectives of the District; or (b) for
17 legitimate business use.
18
19 2. Privileges – The use of the District’s electronic networks is a privilege, not a right, and
20 inappropriate use will result in a cancellation of those privileges. The system administrator
21 (and/or building principal) will make all decisions regarding whether or not a user has
22 violated these procedures and may deny, revoke, or suspend access at any time. His or her
23 decision is final.
24
25 3. Unacceptable Use – The user is responsible for his or her actions and activities involving the
26 network. Some examples of unacceptable uses are:
27
28 a. Using the network for any illegal activity, including violation of copyright or other
29 contracts, or transmitting any material in violation of any federal or state law;
30
31 b. Unauthorized downloading of software, regardless of whether it is copyrighted or
32 devirused;
33
34 c. Downloading copyrighted material for other than personal use;
35
36 d. Using the network for private financial or commercial gain;
37
38 e. Wastefully using resources, such as file space;
39
40 f. Hacking or gaining unauthorized access to files, resources, or entities;
41
42 g. Invading the privacy of individuals, which includes the unauthorized disclosure,
43 dissemination, and use of information of a personal nature about anyone;
44
45 h. Using another user’s account or password;
46

47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92

- i. Posting material authored or created by another, without his/her consent;
 - j. Posting anonymous messages;
 - k. Using the network for commercial or private advertising;
 - l. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
 - m. Using the network while access privileges are suspended or revoked.
4. Network Etiquette – The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:
- a. Be polite. Do not become abusive in messages to others.
 - b. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
 - c. Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.
 - d. Recognize that electronic mail (e-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
 - e. Do not use the network in any way that would disrupt its use by other users.
 - f. Consider all communications and information accessible via the network to be private property.
5. No Warranties – The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or the user’s errors or omissions. Use of any information obtained via the Internet is at the user’s own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.
6. Indemnification – The user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District, relating to or arising out of any violation of these procedures.

- 93
94
95
96 7. Security – Network security is a high priority. If the user can identify a security problem on
97 the Internet, the user must notify the system administrator or building principal. Do not
98 demonstrate the problem to other users. Keep your account and password confidential. Do
99 not use another individual’s account without written permission from that individual.
100 Attempts to log on to the Internet as a system administrator will result in cancellation of user
101 privileges. Any user identified as a security risk may be denied access to the network.
102
- 103 8. Vandalism – Vandalism will result in cancellation of privileges, and other disciplinary action.
104 Vandalism is defined as any malicious attempt to harm or destroy data of another user, the
105 Internet, or any other network. This includes, but is not limited to, the uploading or creation
106 of computer viruses.
107
- 108 9. Telephone Charges – The District assumes no responsibility for any unauthorized charges or
109 fees, including telephone charges, long-distance charges, per-minute surcharges, and/or
110 equipment or line costs.
111
- 112 10. Copyright Web Publishing Rules – Copyright law and District policy prohibit the
113 republishing of text or graphics found on the Web or on District Websites or file servers,
114 without explicit written permission.
115
- 116 a. For each republication (on a Website or file server) of a graphic or text file that was
117 produced externally, there must be a notice at the bottom of the page crediting the
118 original producer and noting how and when permission was granted. If possible, the
119 notice should also include the Web address of the original source.
120
- 121 b. Students and staff engaged in producing Web pages must provide library media
122 specialists with e-mail or hard copy permissions before the Web pages are published.
123 Printed evidence of the status of “public domain” documents must be provided.
124
- 125 c. The absence of a copyright notice may not be interpreted as permission to copy the
126 materials. Only the copyright owner may provide the permission. The manager of the
127 Website displaying the material may not be considered a source of permission.
128
- 129 d. The “fair use” rules governing student reports in classrooms are less stringent and permit
130 limited use of graphics and text.
131
- 132 e. Student work may only be published if there is written permission from both the
133 parent/guardian and the student.
134
- 135 11. Use of Electronic Mail.
136
137
138

- 139
140
141
142 a. The District's electronic mail system, and its constituent software, hardware, and data
143 files, are owned and controlled by the District. The District provides e-mail to aid
144 students and staff members in fulfilling their duties and responsibilities and as an
145 education tool.
146
147 b. The District reserves the right to access and disclose the contents of any account on its
148 system without prior notice or permission from the account's user. Unauthorized access
149 by any student or staff member to an electronic mail account is strictly prohibited.
150
151 c. Each person should use the same degree of care in drafting an electronic mail message as
152 would be put into a written memorandum or document. Nothing should be transmitted in
153 an e-mail message that would be inappropriate in a letter or memorandum.
154
155 d. Electronic messages transmitted via the District's Internet gateway carry with them an
156 identification of the user's Internet "domain." This domain name is a registered domain
157 name and identifies the author as being with the District. Great care should be taken,
158 therefore, in the composition of such messages and how such messages might reflect on
159 the name and reputation of this District. Users will be held personally responsible for the
160 content of any and all electronic mail messages transmitted to external recipients.
161
162 e. Any message received from an unknown sender via the Internet should either be
163 immediately deleted or forwarded to the system administrator. Downloading any file
164 attached to any Internet-based message is prohibited, unless the user is certain of that
165 message's authenticity and the nature of the file so transmitted.
166
167 f. Use of the District's electronic mail system constitutes consent to these regulations.
168

169 Internet Safety
170

- 171 1. Internet access is limited to only those "acceptable uses," as detailed in these procedures.
172 Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed
173 in these procedures, and will otherwise follow these procedures.
174
175 2. Staff members shall supervise students while students are using District Internet access, to
176 ensure that the students abide by the Terms and Conditions for Internet access, as contained
177 in these procedures.
178
179 3. Each District computer with Internet access has a filtering device that blocks entry to visual
180 depictions that are: (1) obscene; (2) pornographic; or (3) harmful or inappropriate for
181 students, as defined by the Children's Internet Protection Act and as determined by the
182 Superintendent or designee.
183
184

185
186
187
188
189
190
191
192
193
194
195
196
197
198

4. The system administrator and building principals shall monitor student Internet access.

Legal Reference: Children’s Internet Protection Act, P.L. 106-554
20 U.S.C. § 6801, et seq.
47 U.S.C. § 254(h) and (l)

Procedure History:
Promulgated on:
Revised: 9-13-05