

1 The [Transylvania County Board of Education \(the “board”\)](#) provides its students and staff access  
2 to a variety of technological resources. These resources provide opportunities to enhance  
3 learning and improve communication within the school community and with the larger global  
4 community. Through the school system’s technological resources, users can observe events as  
5 they occur around the world, interact with others on a variety of subjects, and acquire access to  
6 current and in-depth information.

7  
8 The board intends that students and employees benefit from these resources while remaining  
9 within the bounds of safe, legal, and responsible use. Accordingly, the board establishes this  
10 policy to govern student and employee use of school system technological resources. This  
11 policy applies regardless of whether such use occurs on or off school system property, and it  
12 applies to all school system technological resources, including but not limited to computer  
13 networks and connections, the resources, tools, and learning environments made available by or  
14 on the networks, and all devices that connect to those networks.

15  
16 **A. EXPECTATIONS FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES**

17  
18 The use of school system technological resources, including access to the Internet, is a  
19 privilege, not a right. Individual users of the school system’s technological resources are  
20 responsible for their behavior and communications when using those resources.  
21 Responsible use of school system technological resources is use that is ethical, respectful,  
22 academically honest, and supportive of student learning. Each user has the responsibility  
23 to respect others in the school community and on the Internet. Users are expected to  
24 abide by the generally accepted rules of network etiquette. General student and employee  
25 behavior standards, including those prescribed in applicable board policies, the Code of  
26 Student Conduct, and other regulations and school rules, apply to use of the Internet and  
27 other school technological resources.

28  
29 In addition, anyone who uses school system computers or electronic devices or who  
30 accesses the school network or the Internet using school system resources must comply  
31 with the additional rules for responsible use listed in Section B, below. These rules are  
32 intended to clarify expectations for conduct but should not be construed as all-inclusive.

33  
34 Before using the Internet, all students must be trained about appropriate online behavior  
35 as provided in policy 3226/4205, Internet Safety.

36  
37 All students and employees must be informed annually of the requirements of this policy  
38 and the methods by which they may obtain a copy of this policy. Before using school  
39 system technological resources, students and employees must sign a statement indicating  
40 that they understand and will strictly comply with these requirements and acknowledging  
41 awareness that the school system uses monitoring systems to monitor and detect  
42 inappropriate use of technological resources. Failure to adhere to these requirements will  
43 result in disciplinary action, including revocation of user privileges. Willful misuse may

44 result in disciplinary action and/or criminal prosecution under applicable state and federal  
45 law.

46

47 **B. RULES FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES**

48

49 1. School system technological resources are provided for school-related purposes  
50 only. Acceptable uses of such technological resources are limited to responsible,  
51 efficient, and legal activities that support learning and teaching. Use of school  
52 system technological resources for commercial gain or profit is prohibited.

53 Student personal use of school system technological resources for amusement or  
54 entertainment is also prohibited. Because some incidental and occasional  
55 personal use by employees is inevitable, the board permits infrequent and brief  
56 personal use by employees so long as it occurs on personal time, does not  
57 interfere with school system business, and is not otherwise prohibited by board  
58 policy or procedure.

59

60 2. Under no circumstance may software purchased by the school system be copied  
61 for personal use.

62

63 3. Students and employees must comply with all applicable laws, including those  
64 relating to copyrights and trademarks, confidential information, and public  
65 records. Any use that violates state or federal law is strictly prohibited.  
66 Plagiarism of Internet resources will be treated in the same manner as any other  
67 incidents of plagiarism, as stated in the Code of Student Conduct.

68

69 4. No user of technological resources, including a person sending or receiving  
70 electronic communications, may engage in creating, intentionally viewing,  
71 accessing, downloading, storing, printing, or transmitting images, graphics  
72 (including still or moving pictures), sound files, text files, documents, messages,  
73 or other material that is obscene, defamatory, profane, pornographic, harassing,  
74 abusive, or considered to be harmful to minors.

75

76 5. The use of anonymous proxies to circumvent content filtering is prohibited.

77

78 6. Users may not install or use any Internet-based file sharing program designed to  
79 facilitate sharing of copyrighted material.

80

81 7. Users of technological resources may not send electronic communications  
82 fraudulently (i.e., by misrepresenting the identity of the sender).

83

84 8. Users must respect the privacy of others. When using e-mail, chat rooms, blogs,  
85 or other forms of electronic communication, students must not reveal personal  
86 identifying information or information that is private or confidential, such as the  
87 home address or telephone number, credit or checking account information, or

88 social security number of themselves or fellow students. For further information  
89 regarding what constitutes personal identifying information, see policy  
90 4705/7825, Confidentiality of Personal Identifying Information. In addition,  
91 school employees must not disclose on school system websites or web pages or  
92 elsewhere on the Internet any personally identifiable, private, or confidential  
93 information concerning students (including names, addresses, or pictures) without  
94 the written permission of a parent or guardian or an eligible student, except as  
95 otherwise permitted by the Family Educational Rights and Privacy Act (FERPA)  
96 or policy 4700, Student Records. Users also may not forward or post personal  
97 communications without the author's prior consent.  
98

- 99 9. Users may not intentionally or negligently damage computers, computer systems,  
100 electronic devices, software, computer networks, or data of any user connected to  
101 school system technological resources. Users may not knowingly or negligently  
102 transmit computer viruses or self-replicating messages or deliberately try to  
103 degrade or disrupt system performance. Users must scan any downloaded files  
104 for viruses.  
105
- 106 10. Users may not create or introduce games, network communications programs, or  
107 any foreign program or software onto any school system computer, electronic  
108 device, or network without the express permission of the technology director or  
109 designee.  
110
- 111 11. Users are prohibited from engaging in unauthorized or unlawful activities, such as  
112 "hacking" or using the computer network to gain or attempt to gain unauthorized  
113 or unlawful access to other computers, computer systems, or accounts.  
114
- 115 12. Users are prohibited from using another individual's ID or password for any  
116 technological resource without permission from the individual. Students must  
117 also have permission from the teacher or other school official.  
118
- 119 13. Users may not read, alter, change, block, execute, or delete files or  
120 communications belonging to another user without the owner's express prior  
121 permission.  
122
- 123 14. Employees shall not use passwords or user IDs for any data system (e.g., the state  
124 student information and instructional improvement system applications, time-  
125 keeping software, etc.) for an unauthorized or improper purpose.  
126
- 127 15. If a user identifies a security problem on a technological resource, he or she must  
128 immediately notify a system administrator. Users must not demonstrate the  
129 problem to other users. Any user identified as a security risk will be denied  
130 access.  
131

132 16. Teachers shall make reasonable efforts to supervise students' use of the Internet  
133 during instructional time.

134  
135 17. Views may be expressed on the Internet or other technological resources as  
136 representing the view of the school system or part of the school system only with  
137 prior approval by the superintendent or designee.  
138

139 **C. RESTRICTED MATERIAL ON THE INTERNET**

140  
141 The Internet and electronic communications offer fluid environments in which students  
142 may access or be exposed to materials and information from diverse and rapidly changing  
143 sources, including some that may be harmful to students. The board recognizes that it is  
144 impossible to predict with certainty what information on the Internet students may access  
145 or obtain. Nevertheless school system personnel shall take reasonable precautions to  
146 prevent students from accessing material and information that is obscene, pornographic,  
147 or otherwise harmful to minors, including violence, nudity, or graphic language that does  
148 not serve a legitimate pedagogical purpose. The superintendent shall ensure that  
149 technology protection measures are used as provided in policy 3226/4205, Internet  
150 Safety, and are disabled or minimized only when permitted by law and board policy. The  
151 board is not responsible for the content accessed by users who connect to the Internet via  
152 their personal mobile telephone technology (e.g., 3G, 4G service).  
153

154 **D. PARENTAL CONSENT**

155  
156 The board recognizes that parents of minors are responsible for setting and conveying the  
157 standards their children should follow when using media and information sources.  
158 Accordingly, before a student may independently access the Internet, the student's parent  
159 must be made aware of the possibility that the student could obtain access to  
160 inappropriate material while engaged in independent use of the Internet. The parent and  
161 student must consent to the student's independent access to the Internet and to monitoring  
162 of the student's Internet activity and e-mail communication by school personnel.  
163

164 In addition, in accordance with the board's goals and visions for technology, students  
165 may require accounts in third party systems for school related projects designed to assist  
166 students in mastering effective and proper online communications or to meet other  
167 educational goals. Parental permission will be obtained when necessary to create and  
168 manage such third party accounts.  
169

170 **E. PRIVACY**

171  
172 Students, employees, visitors, and other users have no expectation of privacy in anything  
173 they create, store, send, delete, receive, or display when using the school system's  
174 network, devices, Internet access, email system, or other technological resources owned  
175 or issued by the school system, whether the resources are used at school or elsewhere,

176 and even if the use is for personal purposes. Users should not assume that files or  
177 communications created, transmitted, or displayed using school system technological  
178 resources or stored on servers or on the storage mediums of individual devices will be  
179 private. The school system may, without notice, (1) monitor, track, and/or log network  
180 access, communications, and use; (2) monitor and allocate files server space; and (3)  
181 access, review, copy, store, delete, or disclose the content of all user files, regardless of  
182 medium, the content of electronic mailboxes, and system outputs, such as printouts, for  
183 any lawful purpose. Such purposes may include, but are not limited to, maintaining  
184 system integrity, security, or functionality, ensuring compliance with board policy and  
185 applicable laws and regulations, protecting the school system from liability, and  
186 complying with public records requests. School system personnel shall monitor online  
187 activities of individuals who access the Internet via a school-owned device.  
188

189 By using the school system's network, Internet access, email system, devices, or other  
190 technological resources, individuals consent to have that use monitored by authorized  
191 school system personnel as described in this policy.  
192

#### 193 **F. USE OF PERSONAL TECHNOLOGY ON SCHOOL SYSTEM PROPERTY**

194 Each principal may establish rules for his or her school site as to whether and how  
195 personal technology devices (including, but not limited to smart phones, tablets, laptops,  
196 etc.) may be used on campus. Students' devices are governed also by policy 4318, Use  
197 of Wireless Communication Devices. The school system assumes no responsibility for  
198 personal technology devices brought to school.  
199

#### 201 **G. PERSONAL WEBSITES**

202 The superintendent may use any means available to request the removal of personal  
203 websites that substantially disrupt the school environment or that utilize school system or  
204 individual school names, logos, or trademarks without permission.  
205  
206

##### 207 **1. Students**

208  
209 Though school personnel generally do not monitor students' Internet activity  
210 conducted on non-school system devices during non-school hours, when the  
211 student's online behavior has a direct and immediate effect on school safety or  
212 maintaining order and discipline in the schools, the student may be disciplined in  
213 accordance with board policy (see the student behavior policies in the 4300  
214 series).  
215

##### 216 **2. Employees**

217  
218 Employees' personal websites are subject to policy 7335, Employee Use of Social  
219 Media.

220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248

### 3. Volunteers

Volunteers are to maintain an appropriate relationship with students at all times. Volunteers are encouraged to block students from viewing personal information on volunteer personal websites or online networking profiles in order to prevent the possibility that students could view materials that are not age-appropriate. An individual volunteer's relationship with the school system may be terminated if the volunteer engages in inappropriate online interaction with students.

Legal References: U.S. Const. amend. I; Children's Internet Protection Act, 47 U.S.C. 254(h)(5); Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; 17 U.S.C. 101 *et seq.*; 20 U.S.C. 6777; G.S. 115C-325(e) (applicable to career status teachers), -325.4 (applicable to non-career status teachers)

Cross References: Curriculum and Instructional Guides (policy 3115), Technology in the Educational Program (policy 3220), Internet Safety (policy 3226/4205), Copyright Compliance (policy 3230/7330), Web Page Development (policy 3227/7322), Student Behavior Policies (all policies in the 4300 series), Student Records (policy 4700), Confidentiality of Personal Identifying Information (policy 4705/7825), Public Records – Retention, Release, and Disposition (policy 5070/7350), Use of Equipment, Materials, and Supplies (policy 6520), Network Security (policy 6524), Staff Responsibilities (policy 7300), Employee Use of Social Media (policy 7335)

Adopted: