

## **DIGITAL CITIZENSHIP AND INTERNET ACCEPTABLE USE POLICY**

### **1. Introduction and Purpose**

The Dover Sherborn Public Schools believe in providing all students, staff and teachers with access to electronic resources that promote educational excellence, sharing of information, innovative instruction and online communication. It is our belief that the importance of technology accessibility and access to the abundance of resources on the Internet is critical for delivery of all educational content.

Online access and responsible communication is critical for all learners to apply 21<sup>st</sup>-century skills to keep students safe and comply with the Children's Internet Protection Act (CIPA), the Acceptable Use Policy is put in place, reviewed and approved by School Committee annually to comply with existing law and balance the desire to use technology with the need to protect the Schools from unnecessary liability.

This Acceptable Use Policy is written for all those who use school provided network connections. These connections may be used for educational purposes employing tools such as interactive websites, blogs, podcasts, video conferencing, wikis, and access to E-Learning platforms as well as performing research. The use of these tools must be consistent with the educational objectives of the Schools.

All students, faculty and staff in the Dover Sherborn Public Schools will be provided access to the Internet via a network login using school owned desktops or laptops or via wireless access on any electronic device be it school owned or personally owned. It is understood that all users will have reviewed and adhere to our guidelines for network, Internet and electronic device access.

### **2. Schools' Responsibilities**

In compliance with the Child Internet Protection Act of 2000, which places a duty on the Schools to protect students from inappropriate material on the Internet, the Schools take precautionary measures to protect children from exposure to inappropriate materials, including filtering access to the Internet. The Schools ensure that all school owned computer systems are protected and secure.

All files and messages created, retrieved and/or stored on school equipment using the Schools' network or Internet are the property of the Dover Sherborn Public Schools and should not be considered confidential, consistent with the Electronic Communication Privacy Act. All network and email accounts are provided to all students (grades 6-12), staff, administrators, and faculty and are supported by the IT Department. All email messages created with the school-provided email system are archived for a minimum of seven years. Where appropriate, communications including text and images may be

disclosed to law enforcement or other third parties without prior consent of the sender or receiver.

### **3. User Responsibilities**

All network resources require a network password to access. It is the sole responsibility of the user to keep his/her password secure and to change your password often. If you feel that your password has been compromised, it is your responsibility to notify the IT Department and request a password change.

It is a violation of this agreement for any user to share/use his/her password.

## **Digital Responsibility**

### **4. Online/Network Etiquette**

*Users* are expected to learn and to abide by generally accepted rules of online network etiquette, as well as rules of schools' handbooks. These include respect and responsibility as well as avoidance of vulgar language. Try to avoid sarcasm and humor; without face-to-face communication, your *comments* may be misinterpreted or viewed as criticism. Harassing, bullying, swearing, vulgarities, suggestive, obscene, threatening or abusive language of any kind is not acceptable. Online access is not allowed to make or distribute jokes or stories, cyberbully, obscene material or material that is based on inappropriate remarks or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientations.

**5. Websites, Social Networking, blogging, wikis, podcasting, video or other Web 2.0 tools** are considered an extension of classroom collaboration and communication. Whether at school or home, any speech that is considered inappropriate in the classroom is also inappropriate in all use of blogs, wikis, podcasts and other Web 2.0 tools. Students using these communication tools are expected to act safely by keeping all personal information out of their posts. Comments made on school related blogs should follow the rules of online etiquette described above and will be monitored by school personnel. If comments or posts are inappropriate, they will be deleted.

### **6. Messaging/Email**

Teachers may incorporate: email, blogs, podcasts, video conferencing, online collaborations, instant messaging, texting, Virtual Learning Environments and other forms of direct electronic communications (i.e. cell phones, PDAs, cameras) or Web 2.0 applications for educational purposes. Although teachers monitor student online activity, it is the direct responsibility of the user to comply with this Acceptable Use Policy.

### **7. Plagiarism**

Plagiarism is the act of using someone else's words or ideas as your own. Students are required to give proper credit to all Internet sources used in academic assignments, whether quoted or summarized. This includes all forms of media on the Internet, such as, but not limited to, graphics, movies, music, and text. Plagiarism of Internet resources will be dealt with consistent with existing disciplinary guidelines relating to plagiarism.

## **8. Copyright/Licensing**

The Schools strongly condemn the illegal distribution (otherwise known as pirating) of software; making available copyrighted software or other content that has had the copyright protection removed; making available serial numbers for software that can be used to illegally validate or register software; making available tools that can be used for no purpose other than for "cracking" software or other copyrighted content. Abuse in this area may result in suspension or termination of network access privileges and may also result in other disciplinary action consistent with the disciplinary policies of the Schools. In addition, if such conduct constitutes a violation of law, criminal prosecution may result. All users should be aware that software piracy is a federal offense and is punishable by a fine or imprisonment.

## **9. Proxies**

The use of anonymous proxies to circumvent the content filter is strictly prohibited and is a direct violation of this agreement. If you have a legitimate reason to believe that a site being blocked should be unblocked, please submit the URL of the blocked site to the IT Department for review.

## **10. Additional Illegal Activities**

Use of the network for any illegal activities is prohibited. Illegal activities include, but are not limited to: (a) tampering with computer hardware or software, (b) unauthorized entry into computers and files (hacking), (d) knowledgeable vandalism or destruction of equipment, (e) deletion of computer files belonging to someone other than oneself, (f) gambling, (g) posting inappropriate content (including but not limited to images, video, audio and comments) can result in disciplinary consequences as well as potential legal charges. Users must be aware that any illegal action carried out over the Internet will be reported to law enforcement officials for possible prosecution. Please be advised, it is a federal offense (felony) to break into any security system. Financial and legal consequences of such actions are the responsibility of the user and student's parent or guardian.

## **11. Bullying & Cyberbullying**

**Please see the *Dover Sherborn Public Schools Bullying Prevention-Intervention Plan* found at**

**[www.doversherborn.org](http://www.doversherborn.org) or available in hard copy at any school.**

- a. **Bullying**, as defined in M.G.L. c. 71, § 37O is the repeated use by one or more students of a written, verbal or electronic expression or a physical act or gesture or any combination thereof, directed at a target that:
  1. causes physical or emotional harm to the target or damage to the target's property;
  2. places the target in reasonable fear of harm to himself or herself or of damage to his or her property;
  3. creates a hostile environment at school for the target;
  4. infringes on the rights of the target at school; or

5. materially and substantially disrupts the education process or the orderly operation of a school.
- b. Cyberbullying is bullying through the use of technology or electronic devices such as telephones, cell phones, computers, and the Internet. It includes, but is not limited to, email, instant messages, text messages, and Internet postings. See M.G.L. c. 71, § 37O for the legal definition of cyberbullying.
- c. Hostile environment, as defined in M.G.L. c. 71, § 37O, is a situation in which bullying causes the school environment to be permeated with intimidation, ridicule or insult that is sufficiently severe or pervasive to alter the conditions of a student's education.

## **12. Terms and Conditions**

The Schools reserve the right to deny, revoke or suspend specific user privileges and or to take other disciplinary action, up to and including suspension, expulsion (students), or dismissal (staff) for violations of these Guidelines. The District will advise appropriate law enforcement agencies of illegal activities conducted through the Dover Sherborn Network Connection. The Schools also will cooperate fully with local, state, and/or federal officials in any investigation related to any illegal activities conducted through the service.

School administration reserves the right to amend this policy at any time without prior notice.

### **Personal Electronic Devices (PEDs)**

**PED Definition:** Personal Electronic Devices whose main purpose are for personal entertainment and/or communication, such as, but not limited to: cell phones (such as, but not limited to, smart phones, feature phones, dumb phones), iPods, iPads, digital cameras, video cameras, MP3 players, laptops, netbooks, and e-Readers (such as, but not limited to, Kindles and Nooks) that are student-owned.

**PED Overview:** Increased student use of school and personal electronic devices (PEDs) has the potential for both positive and negative consequences. PEDs can help to enhance the learning environment, and many schools have incorporated them in teaching and learning with much success. However, student use of PEDs can be abused in such a way that it negatively affects students, teachers, and the overall school environment. This policy is intended to support the benefits of PEDs use while curtailing possible abuses.

**PED Unacceptable Use:** The following behaviors related to the use of PEDs are unacceptable at all times: making threats, cyber-bullying, taking photos without first obtaining the written consent from the individuals involved before taking photos, taking

videos without first obtaining the written consent from the individuals involved before the recording of sound or video, sexting, plagiarism, cheating, copyright violation. Engaging in these types of behaviors can result in disciplinary consequences as well as potential legal charges.

**PED Classroom Standards:** Teachers will select a classroom standard regarding the use of PEDs in his or her classroom. Each teacher (and other staff such as, but not limited to the librarian and nurse) will select a PED Usage Level for his or her classroom (or specific section of the school campus - the auditorium, cafeteria, library or nurses room for example) and communicate expectations clearly to the students as well as consequences should there be a violation from the designated standard. The PED Usage Levels are as follows:

- **PED Usage Level 1:** Personal Electronic Devices (PEDs) are not allowed in this classroom.
- **PED Usage Level 2:** Personal Electronic Devices (PEDs) are sometimes allowed in this classroom based on the curriculum for that course. In addition, certain features of various PEDs may be allowed while other features may not be allowed. For example, the iPod feature of a cell phone may be allowed but the texting feature of a cell phone may not be allowed.
- **PED Usage Level 3:** Personal Electronic Devices (PEDs) are always allowed in this classroom based on the curriculum for that course.

**Responsibility:** Students who bring PEDs to school do so at their own risk. It is the responsibility of the students to treat their PEDs with respect and to protect them to prevent theft or damage.

**Off Campus:** The Acceptable Use Policy for PEDs also applies to students during off-campus school events. These events include but are not limited to, athletic events, field trips, camps and other extra-curricular activities.

**Emergency Situations:** During fire drills, emergency situations when being spoken to by an adult, the student should remove both “ear buds” and address the adult or situation at hand.

**Tests and Exams:** All PEDs must be switched off during tests and other exams. Failure to do so may be regarded as cheating.

**Assemblies:** All PEDs must be switched off during assemblies and other events such as, but not limited to, listening to a guest speaker in a classroom.

**PED Violations:** Students and parent(s)/guardian(s) should consult with their child’s school’s handbook for information regarding violations,

The Schools reserve the right to amend this policy at any time without prior notice.

FIRST READING: January 25, 2011

SECOND READING: May 22, 2012

ADOPTED: May 22, 2012

SOURCE:

**USER CONTRACT**

I understand and will abide by the Digital Citizenship and Internet Acceptable Use Policy. I have received a copy of the Policy and am aware there is a copy of the document maintained on the Dover-Sherborn Public Schools web site. I further understand that any violation by me of the terms of the Policy may result in the suspension or revocation of my Network and/or Internet privileges and may also result in school disciplinary action. If a violation constitutes a criminal offense, appropriate legal action may be taken. I further agree to indemnify the Dover-Sherborn Public Schools for any losses, costs or damages, including reasonable attorney's fees, incurred by the Dover-Sherborn Public Schools relating to or arising out of any violation by me of the Network and Internet Acceptable Use Policy.

Name (please print)

---

Date: \_\_\_\_\_ Signature: \_\_\_\_\_

---

**PARENT/GUARDIAN CONTRACT  
(for Users under 18 Years of Age)**

Student's

Name:

---

As parent/guardian of the above-named student, I have read the Network and Internet Acceptable Use Policy. I understand that this access is designed for educational purposes. I recognize that some controversial materials exist on the Internet. I have discussed with my son/daughter his/her responsibilities regarding the use of the Dover-Sherborn Public Schools' Network and Internet access. My son/daughter understands and agrees to follow the Network and Internet Acceptable Use Policy of the Dover-Sherborn Public Schools. I understand that any violation by my son/daughter of the terms of the Network and Internet Acceptable Use Policy may result in the suspension or revocation of his/her Network and/or Internet privileges and may also result in school disciplinary action. I will not hold the Dover-Sherborn Public Schools liable or responsible for any materials my son/daughter accesses, acquires or transmits via the Dover-Sherborn Public Schools' computer network and/or Internet connection. I hereby give permission for my son/daughter to use the Network and Internet at school. I further agree to indemnify the Dover-Sherborn Public Schools for any losses, costs or damages, including reasonable attorney's fees, incurred by the Dover-Sherborn Public Schools relating to or arising out of any violation by my son/daughter of the Network and Internet Acceptable Use Policy.

Parent/Guardian Name (please print)

---

Date \_\_\_\_\_ Signature: \_\_\_\_\_

---