2295 Acceptable Computer, Network and Internet Use Policy 2295

The Milford School District provides students and staff access to various technologies and the internet to use for teaching, learning or other school district business. The opportunity to use the network goes “hand in hand” with the responsibility to use computers and the internet properly. Access is a privilege, not a right, and that access requires responsibility. Safe and responsible use of the internet and the devices that connect to it is a priority of the Milford School District.

For purposes of this policy, "user” means any person authorized to access personal or School District computer systems and wired or wireless networks including, but not limited to, the Internet. Users are expected to demonstrate ethical behavior that is of the highest order when using technologies and when accessing the internet for teaching, learning and other school district business. Users are also expected to follow all guidelines stated in this policy as well as any additional guidance provided verbally or in writing by IT staff, teachers or administration.

Use of the Internet

Resources available on the internet vary in quality and appropriateness for school purposes; therefore, it is important that all users make sure that internet materials and information are school appropriate. Unlike other teaching and learning materials, the very nature of the internet may not allow for the same formal selection processes for internet resources as for textbooks and library resources, so the responsibility for appropriateness rests with users.

The use of the internet by students is for research and other educational purposes as assigned by a teacher or related to school curriculum and activities. Within the guidelines of the Children’s Internet Protection Act (CIPA), freedom of speech and access to information will be honored.

Activities not permitted include, but are not limited to:

1. Sending or displaying offensive messages or pictures
2. Using obscene or offensive language
3. Harassing, insulting, or attacking others online or any other behavior that can be considered bullying
4. Damaging or disabling computers, computer systems or computer networks or bypassing or compromising the function of the internet content filtering systems
5. Violating copyright laws
6. Using others’ passwords, name or accounts
7. Trespassing in others’ folders, work or files
8. Engaging in illegal activities
9. Hacking of any kind
10. Soliciting or proselytizing for commercial ventures, political or religious causes, outside organizations or other non-School business related purposes

11. Loading or downloading non-approved software applications like screensavers, games, graphics/multimedia utilities, etc. onto school computers
12. Loading, downloading or accessing any content prohibited in an educational setting as determined by the Superintendent/designee.

Internet Safety

The Children's internet Protection Act (CIPA) and the Protecting Children in the 21st Century Act mandate specific strategies to foster safe and responsible use of technologies and to prevent adverse computer and internet use by school-age children. The District will allow students and staff to access instructional resources and information from the internet using District technologies and networks while protecting them from cybercrime and information inappropriate for minors. It will take the following steps to promote safe and appropriate online behavior:

1. **Internet Policy agreement**
   This internet policy will be provided in staff and student/parent handbooks. Users will be required to agree to adhere to the policy with a signature on an annual acknowledgement form and each time they sign onto the network by accepting the electronic acceptable use reminder.

2. **Content filtering**
   The District will use a content filtering package prescribed by and compliant with CIPA to block obscenity, pornography and other sites deemed harmful to minors. While the District will make every effort to choose and use appropriate filtering software, it recognizes that filtering is not 100% effective and cannot guarantee that all objectionable material will be blocked. The District also recognizes that the filter may block legitimate material that the student may be able to access outside of school.

3. **Supervision and monitoring**
   Teachers and staff will monitor, within reason, the use of computers, other technologies and the internet. During school, teachers will guide students toward appropriate materials. Administrators, or their designees, may review files and communications (including electronic mail) without notice to ensure that users are using the system responsibly. Users should not have the expectation that District-managed files and information are private.

Search of Social Media Accounts

School personnel are permitted to investigate alleged misconduct based on activity associated with a student's social media account. During the investigation into a student's alleged misconduct, school officials may request that a student VOLUNTARILY share a printed copy of specific communication from the student's social media account that is relevant to the ongoing investigation.

School personnel **shall not**:

- Require or request a student or a prospective student to disclose or to provide access to personal social media accounts through the student's user name, password or other means of authentication that provides access.
- Require or request a student or a prospective student to access a personal social media account in the presence of a school employee in a manner that allows the employee to observe the social media account
- Compel a student to add anyone to the list of contacts associated with his or her social media account
- Require, request, suggest, or cause a student to change the privacy settings associated with a personal social media account
- Take action or threaten to take action against a student for refusing to disclose information related to social media accounts.

Instruction

The District will develop and implement Information and Technology Literacy curriculum and instruction that promotes safe and appropriate online behavior, including interacting with others through social networking websites, chat rooms and other forms of messaging, and cyberbullying awareness and response.

Policy Violations

Any actions that might harm computer equipment, software, data, another user, or the internet, or that show disregard for the proper procedures set up for network access will not be tolerated. Violations of this policy may result in restrictions or suspension of the user's technology use or network privileges, disciplinary action, and/or legal action in accordance with the law, Board policy and administrative regulations. Further, any users of the School District's computer systems or networks who intentionally violate the District's policy and who intentionally damage the computer systems or network or misuse the internet shall assume legal and financial liability for such damage.

Approved: 9/1996
Revised: 5/2000, 1/2002, 5/2002, 6/2010, 2/2012, 1/2016, 5/2016

Reference:
Child Internet Protection Act, 2000.
Protecting Children in the 21st Century Act.
Milford School District Policy # 2296, Copyright Compliance Policy.
Milford School District Policy # 5009, Pupil Safety and Violence
Prevention – Bullying.
RSA 189:70