Yarmouth School Department
Internet Acceptable Use Policies
for Student and Staff

Introduction
Yarmouth has had an Internet Acceptable Use Policy Since 1996. Recent case law and advice from our school attorneys prompted the School Committee to update the policies in January 2008. We now have separate staff and student policies. The policies apply to all visitors who use our equipment. A signature is not necessary for the policy to be binding on all users.

Table of Contents

I. STUDENT TECHNOLOGY AND INTERNET USE

NEPN/NSBA Code: IJNDB

The Yarmouth School Department provides technology, networks, and Internet access to support the educational mission of the school and to enhance teaching and learning opportunities for students and school staff. The School Committee believes that the resources available through the Internet are of significant value in the learning process and preparing students for future success. At the same time, the unregulated availability of information and communication of the Internet requires that schools establish reasonable controls for lawful, efficient and appropriate use of this technology.

Student use of school technology, networks and Internet services is a privilege and not a right. Students are required to comply with this policy and the accompanying rules (IJNDB-R). Students who violate the policy and/or rules may have their technology privileges revoked and may also be subject to further disciplinary and/or legal action.

All Yarmouth School Department technologies remain under the control, custody, and supervision of the school unit. The school unit reserves the right to monitor all technology and Internet activity by students. Students should have no expectation of privacy in their use of school technology.

While reasonable precautions will be taken to supervise student use of the Internet, the Yarmouth School Department cannot reasonably prevent all inappropriate uses, including access to objectionable material and communication with persons outside

of the school, in violation of Board policies/procedures and school rules. The school department is not responsible for the accuracy or quality of information that students obtain through the Internet.

The Superintendent shall be responsible for overseeing the implementation of this policy and accompanying rules and for advising the School Committee of the need for any future amendments or revisions to the policy/rules. The Superintendent may develop additional administrative procedures/rules governing the day-to-day management and operations of the school's computer system as long as they are consistent with the School Committee's policy/rules. The Superintendent may delegate specific responsibilities to building principals and others, as he/she deems appropriate.

Cross Reference:

GCSA Employee Technology and Internet Use

IJNDB-R Student Technology and Internet Use Administrative Procedure

APPROVED: August 29, 1996

REVISED: January 13, 2000, December 12, 2002, January 10, 2008

Student Technology and Internet Use Administrative Procedure

NEPN/NSBA Code: IJNDB-R

This administrative procedure implements School Committee policy IJNDB - Student Technology and Internet Use. This procedure is intended to provide general guidelines and examples of prohibited uses but does not attempt to state all required or prohibited activities by users. Failure to comply with School Committee policy IJNDB and this Administrative Procedure may result in loss of technology and Internet access privileges, disciplinary action and/or legal action.

A. Technology Use is a Privilege, Not a Right

> Student use of the school unit's technology, networks and Internet services is a privilege, not a right. Unacceptable use/activity may result in suspension or cancellation of privileges as well as additional disciplinary and/or legal action.

B. Acceptable Use

Student access to the school units technology, networks and Internet services are provided for educational purposes and research consistent with the school unit's educational mission, curriculum and instructional goals.

The same rules and expectations govern student use of technology as apply to other student conduct and communications.

Students are further expected to comply with these administrative procedures and all specific instruction from the teacher or other supervising staff member/ volunteer with accessing the school unit's computers, networks and Internet services.

C. Prohibited use

The user is responsible for his/her actions and activities involving school unit technology, networks and Internet services and for his/her technology files, passwords and accounts. Examples of unacceptable uses that are expressly prohibited include but are not limited to the following:

1. Accessing Inappropriate Material - Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal.

2. Illegal Activities - Using the school unit's technology, networks and/or Internet services for any illegal activity or activity that violates other School Committee policies, procedures and/or school rules.

3. Violating Copyrights - Copying or downloading copyrighted materials without the owner's permission or any other activity that violates other School committee policies regarding copyright material.

4. Plagiarism - Representing as one's own work any materials obtained on the Internet (such as term papers, articles, etc.). When Internet sources are used in student work, the author, publisher and Web site must be identified.

5. Copying Software - Copying or downloading software without the express authorization of the system administrator.

6. Non-School-Related Uses - Using the school unit's technology, networks and Internet services for non-school-related purposes such as private financial gain, commercial, advertising or solicitation purposes.

7. Misuse of Passwords/Unauthorized Access - Sharing passwords, using other users' passwords without permission and/or accessing other users' accounts.

8. Malicious Use/Vandalism - Any malicious use, disruption or harm to the school unit's technology, networks and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses.

9. Unauthorized Access to Internet Communication Tools - Accessing chat rooms or news groups without specific authorization from the supervising teacher.

D. No Expectation of Privacy

The school unit retains control, custody and supervision of all technology, networks and Internet services owned or leased by the school unit. The school unit reserves the right to monitor all technology and Internet activity by students. Students have no expectations of privacy in their use of school technology, including e-mail and stored files.

E. Compensation for Losses, Costs and/or Damages

The student and/or the student's parent/guardian shall be responsible for compensating the school unit for any losses, costs or damages incurred by the school unit related to violations of policy IJNDB and/or these administrative procedures, including investigation of violations.

F. School Unit Assumes No Responsibility for Unauthorized Charges, Costs or Illegal Use

The school unit assumes no responsibility for any unauthorized charges made by students including but not limited to credit card charges, long distance telephone charges, electronic payment services, equipment and line costs, or for any illegal use of its computers such as copyright violations.

G. MLTI Laptop Home Use

Students may take their laptop home provided the conditions and procedures outlined in the document Laptop Home Use Procedure (IJNDB-E1) are followed.

H. Student Security

A student shall not reveal his/her full name, address, or telephone number on the Internet without prior permission from a supervising teacher. Students should never meet people they have contacted through the Internet without parental permission. Students should inform their supervising teacher if they access information or messages that are dangerous, inappropriate or make them uncomfortable in any way.

I. System Security

The security of the school unit's technology, networks and Internet services is a high priority. Any user who identifies a security problem must notify the technology coordinator. The user shall not demonstrate the problem to others. Any user who attempts or causes a breach of system security shall have his/her privileges revoked and may be subject to additional disciplinary and/or legal action.

reference: IJNDB-E Student Technology Use

Adopted: August, 1996

Revised: January 13, 2000, December 12, 2002, January 10, 2008

II. MLTI Laptop Home Use Procedures

NEPN/NSBA Code: IJNDB-E1

The Yarmouth School Department strongly believes in the power of 1:1 computing in grades 7 through 12. A laptop is being provided. The intent of this initiative is to provide student access to this technology at home as well as at school. In order for this to happen, the following guidelines have been developed and adopted by our school committee:

Guidelines:

1. In order to bring a computer home, parents and students must attend a Family Orientation meeting offered by the school.

2. It is the responsibility of the student and parents to know the guidelines attached to this document. Guidelines are reviewed when students receive the laptop and when parents attend the mandatory orientation session.

3. The Student Acceptable Use Policy applies to home use of school issued laptops.

4. The laptop issued to each student is an educational tool and should only be used in that capacity. Students should have no expectations of privacy in their use of the laptop computer.

5. When the laptop is brought home by the student, it is the expectation that it will be used in a common family location so that adult supervision can be maintained. Parents/ Guardians have the right to their child's login password in order to facilitate in the supervision of the student's computer usage at home.

6. Replacement costs and/or the repair for damages that are not covered by the warranty and that occur to the laptop and its carrying case are the sole responsibility of the undersigned parent/guardian.

7. If the laptop is stolen it should be reported to the Yarmouth Police Department and the principal or assistant principal.

8. Laptops taken out of state are not covered by Apple for any kind of loss or damage.

Cross Reference:

IJNDB Student Technology & Internet Use

APPROVED: December 12, 2002

REVISED: January 10, 2008

III. EMPLOYEE TECHNOLOGY AND INTERNET USE

NEPN/NSBA Code: GCSA

The Yarmouth schools provide technology, networks and Internet access to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students and school staff.

Employees are to utilize the school unit's hardware, software, networks and Internet services for school-related purposes and performance of job duties. Incidental personal use of school technology is permitted as long as such use does not interfere

with the employee's job duties and performance, with the system operations or other system users. “Incidental personal use” is defined as use by an individual employee for occasional personal communications. Employees are reminded that such personal use must comply with this policy and all other applicable policies and administrative procedures.

Any employee who violates this policy and/or any administrative procedures governing use of the school unit's computers will be subject to disciplinary action, up to and including discharge. Illegal uses of the school unit's technology will also result in referral to law enforcement authorities.

All Yarmouth schools technology remain under the control, custody and supervision of the school unit. The school unit reserves the right to monitor all technology and Internet activity by employees. Employees have no expectation of privacy in their use of school technology.

The Superintendent shall be responsible for overseeing the implementation of this policy and the accompanying administrative procedures and for advising the School Committee of the need for any future amendments or revisions to the policy/ administrative procedures. The Superintendent may develop additional administrative procedures governing the day-to-day management and operations of the school unit's technology system as long as they are consistent with the School Committee's policy/ administrative procedure. The Superintendent may delegate specific responsibilities to building principals and others as he/she deems appropriate.

Cross Reference:

GCSA-R - Employee Technology and Internet Use Administrative Procedure

IJNDB - Student Technology and Internet Use

INNDB-R - Student Technology and Internet Use Administrative Procedure

Adopted: January 13, 2000

Revised: January 10, 2008

III. EMPLOYEE TECHNOLOGY AND INTERNET USE ADMINISTRATIVE PROCEDURE

NEPN/NSBA Code: GCSA-R

The intent of this School Committee-level administrative procedure is to provide employees with general requirements for utilizing the school unit's technology, networks and Internet services. The School Committee's administrative procedure may be supplemented by more specific administrative procedures governing day-to-day management and operation of the technology system.

This administrative procedure provides general guidelines and examples of prohibited uses for illustrative purposes but does not attempt to state all required or prohibited activities by users. Employees who have questions regarding whether a particular activity or use is acceptable should seek further guidance from the technology coordinators.

Failure to comply with School Committee policy GCSA, this administrative procedure and/or other established procedures or rules governing technology use may result in disciplinary action, up to and including discharge. Illegal uses of the school unit's technology will also result in referral to law enforcement authorities.

A. Access to School Technology, Networks and Internet Services

The level of access that employees have to school unit computers, networks and Internet services is based upon employee job requirements and needs.

B. Acceptable Use

Employee access to the school unit's technology, networks and Internet services is provided for administrative, educational, communication and research purposes consistent with the school unit's educational mission, curriculum and instructional goals. General rules and expectations for professional behavior and communication apply to the use of the school unit's technology, networks and Internet services.

Employees are to utilize the school unit's technology, networks and Internet services for school-related purposes and performance of job duties. Incidental personal use of school technology is permitted as long as such use does not interfere with the employee's job duties and performance, with system operations or other system users. "Incidental personal use" is defined as use by an individual employee for occasional personal communications. Employees are reminded that such personal use must comply with this policy and all other applicable policies, procedures and rules.

C. Prohibited Use

The employee is responsible for his/her actions and activities involving school unit technology, networks and Internet services and for his/her technology files, passwords and accounts. General examples of unacceptable uses which are expressly prohibited include but are not limited to the following:

1. Any use that is illegal or in violation of other School Committee policies, including harassing, discriminatory or threatening communications and behavior, violations of copyright laws, etc.

2. Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive

3. Any inappropriate communications with students or minors

4. Any use for private financial gain, or commercial, advertising or solicitation purposes except for the "ads and notes" forum available to school employees

5. Any use as a forum for communicating by e-mail or any other medium with other school users or outside parties to solicit, proselytize, advocate or communicate the views of an individual or non-school-sponsored organization; to solicit membership in or support of any non-school-sponsored organization; or to raise funds for any non-school-sponsored purpose, whether for-profit or not-for-profit. No employee shall knowingly provide school e-mail addresses to outside parties whose intent is to communicate with school employees, students and/or families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the building principal or other appropriate administrator

6. Any communication that represents personal views as those of the school unit or that could be misinterpreted as such

7. Downloading or loading software or applications without permission from the system administrator

8. Opening or forwarding any e-mail attachments (executable files) from unknown sources and/or that may contain viruses

9. Any malicious use or disruption of the school unit's technology, networks and Internet services or breach of security features

10. Any misuse or damage to the school unit's technology equipment

11. Misuse of the technology passwords or accounts (employee or other users)

12. Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct

13. Any attempt to access unauthorized sites

14. Failing to report a known breach of technology security to the system administrator

15. Using school technology, networks and Internet services after such access has been denied or revoked

16. Any attempt to delete, erase or otherwise conceal any information stored on school technology that violates these rules

D. No Expectation of Privacy

The school unit retains control, custody and supervision of all technology, networks and Internet services owned or leased by the school unit. The school unit reserves the right to monitor all technology and Internet activity by employees and other system users. Employees have no expectation of privacy in their use of school technology, including e-mail messages and stored files.

E. Confidentiality of Information

Employees are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential.

F. Staff Responsibilities to Students

Teachers, staff members and volunteers who utilize school technology for instructional purposes with students have a duty of care to supervise such use. Teachers, staff members and volunteers are expected to be familiar with the school unit's policies and administrative procedures concerning student technology and Internet use and to enforce them. When, in the course of their duties, employees/volunteers become aware of student violations, they are expected to stop the activity and inform the building principal.

G. Compensation for Losses, Costs and/or Damages

The employee shall be responsible for any losses, costs or damages incurred by the school unit related to violations of policy GCSA and/or this

administrative procedure.

H. School Unit Assumes No Responsibility for Unauthorized Charges, Costs or Illegal Use

The school unit assumes no responsibility for any unauthorized charges made by employees including but not limited to credit card charges, electronic payment services, subscriptions, long distance telephone charges, equipment and line costs, or any illegal use of its computers such as copyright violations.

Cross Reference: GCSA - Employee Technology and Internet Use

IJNDB - Student Technology and Internet Use

IJNDB-R Student Technology and Internet Use Administrative Procedure

Adopted: January 13, 2000

Revised: January 10, 2008

EMPLOYEE USE OF SOCIAL AND EDUCATIONAL NETWORKING SITES

NEPN/NSBA Code: GBEBD

The Yarmouth School Committee recognizes that technological resources enhance employee performance by offering effective tools to assist in providing a quality instructional program and facilitating communications with parents/guardians, students and the community. Employees shall be responsible for the appropriate use of technology both when the technology tools are provided by the district and when any use of technology interacts with students and other staff members.

Educational networking sites, including educational wikis, specially created Nings, or others, enable ongoing communication purposely designed for educational use. Social networking sites, including Facebook, MySpace, among others, are used primarily for personal social interactions. School district employees are prohibited from engaging in any conduct on social or educational networking sites that violates the law, School Committee policies, or other standards of conduct. Additionally, the School Committee developed the following expectations and recommendations for the use of these technology tools to ensure positive professional relationships between students and district staff, to model good online behavior for students, and to

protect students from inappropriate content:

Staff members using social networking sites shall:

- Not accept current Yarmouth students (once students have graduated they are no longer “current” students) as friends on personal social networking sites.
- Decline any student-initiated friend requests.
- Not initiate friendships with students.
- Not post confidential information about students, staff or district business.

Recommendations for the use of social networking sites by staff members:

- Visit your profile’s security and privacy settings. At a minimum, staff members should have all privacy settings set to “only friends” so that your content is not open to a large group of unknown people.
- Since people classified as “friends” have the ability to download and share your information with others, post only what you want the world to see.
- While you have a right to free expression, do consider more effective means of dialogue before using social networking sites to discuss student issues or publicly criticize school policies or personnel.

Staff members using educational networking sites shall:

- Let your administrator, fellow teachers, and parents know about your educational network.
- Have a clear statement of purpose and outcomes for the use of the networking tool.
- Establish a code of conduct for all network participants. The principal at each school will be responsible for providing sample codes of conduct.
- Not post images that include students without parental permission.
- Pay close attention to the site’s security settings and allow only approved participants access to the site.

Recommendations for the use of educational networking sites by staff members:

- When available, use school-supported networking tools.
- Do not say or do any thing that you would not say or do as a teacher in the classroom or as a staff member performing his or her duties.

Cross Reference: GCSA, GCSA-R

Adopted: June 11, 2010