EGA

BARNSTEAD SCHOOL DISTRICT

ACCEPTABLE USE OF E-RESOURCES POLICY

This policy applies to all persons accessing or using school E-resources. This includes school students, faculty and staff, authorized school guests, and all persons authorized for access or use privileges by the school, hereafter referred to as users.

Resources covered

E-resources covered by this policy include, without limitation:

1. all school owned, operated, leased or contracted computing, networking, telephone and information resources, whether they are individually controlled, shared, standalone or networked,

2. all information maintained in any form and in any medium within the school's computer resources, and

3. all school voice and data networks, telephone systems, telecommunications infrastructure, communications systems and services, and physical facilities, including all hardware, software, applications, databases, and storage media.

Additionally, all creation, processing, communication, distribution, storage, and disposal of information by any combination of school E-resources and non-school resources are covered by this policy.

Policy application

Individual areas (e.g., departments and divisions) within the school may define supplemental policies or conditions of acceptable use for E-resources under their control. These additional policies or conditions must be consistent with this policy but may provide additional detail, guidelines and/or restrictions. This policy will supersede any inconsistent provision of any unit policy or condition.

I. USE OF E-RESOURCES

Confidentiality

All users with access to confidential data are to utilize all appropriate precautions to maintain the accuracy, integrity, and confidentiality of the data and ensure that no unauthorized disclosures occur.

Expectation of Privacy

User’s rights

The school provides electronic resources to users to effectively perform their job duties. The school will not routinely monitor an individual user's electronic data, software, or communication files.

School processes

Users should be aware that electronic data, software, and communications files are copied to backup tapes and stored. Items that were deleted may be preserved on backup tapes and retrieved if necessary. All activity on systems and networks may be monitored, logged, and reviewed by system administrators, or discovered in legal proceedings. In addition, all documents created, stored, transmitted or received on school computers and networks may be subject to monitoring by systems administrators.

School rights

The school reserves the right to access, monitor and disclose the contents and activity of an individual user's account(s) and to access any school-owned E-resources and any non-school-owned E-resources, on school property, connected to school networks. This action may be taken to maintain the network's integrity and the rights of others authorized to access the network. Additionally, this action may be taken if the security of a computer or network system is threatened, other misuse of school resources is suspected, or the school has a legitimate business need to review such files (e.g., due to sudden death or incapacity of the employee).

E-Resource Use

All users have the following:

Rights

1. All users are granted access to and permitted use of the school's E-resources. Access is granted for specific purposes based on the user's particular needs or classification.
2. Users have the authority to read, write, edit, or delete information in files or databases, as established by the designated owners of the information.
3. All users are provided with the school's on-campus network access including, electronic mail ("email") and Internet access.

Responsibilities

Each user shall:

1. be responsible for the security and integrity of information stored on his or her personal desktop system. This includes:
   - making regular backups of information and files,
   - controlling and securing physical and network access to E-resources and data,
   - properly logging out of sessions,
   - monitoring access to their accounts, if a user suspects that their access codes have been compromised or that there has been unauthorized activity on their accounts, they are to report it toTech Support and change access codes immediately, and
   - choose appropriate password(s), and guard the security of that password.

  - use only the access codes and privileges associated with their computer account(s) and utilize those account(s) for the purposes for which they were authorized.
  - take full responsibility, when sharing access codes and user account information, for the use of any user to whom they provided their access code.
  - respect and honor the rights of other individuals, with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright infringement, and use of E-resources.

Restrictions
Users may not do the following:

1. Provide access codes to any non-user.
2. Provide access codes to any user not authorized for such access.
3. Make use of accounts, access codes, privileges or E-resources to which they are no longer authorized.
4. Tamper with, modify, or alter restrictions or protection placed on their accounts, the school system, or network facilities.
5. Extend the network by introducing a hub, switch, router, wireless access point, or any other service or device that provides more than one device to the school network.
6. Use the school's Internet access in a malicious manner to alter or destroy any information available on the Internet or on any network accessible through the Internet for which he or she does not own or have explicit permission to alter or destroy.
7. Remote access authentication must not be shared with other users or non-users.
8. Knowingly introduce, create or propagate computer viruses, worms, Trojan Horses, or other malicious code to school E-resources.
9. Use knowledge of security or access controls to damage computer and network systems, obtain extra E-resources, or gain access to accounts for which they are not authorized.
10. Eavesdrop or intercept transmissions not intended for them.
11. Physically damage or vandalize E-resources
12. Attempt to degrade the performance of the system or to deprive authorized users of E-resources or access to any school E-resources.
13. Alter the source address of messages, or otherwise forging email messages.
14. Send email chain letters or mass mailings for purposes other than official school business.

15. Engage in activities that harass, degrade, intimidate, demean, slander, defame, interfere with, or threaten others.

16. Comment or act on behalf of the school over the Internet unless you have the authority to do so.

Copyrights and licenses

Software may not be copied, installed or used on school E-resources except as permitted by the owner of the software and by law. Software, subject to licensing, must be properly licensed and all license provisions (including installation, use, copying, number of simultaneous users, terms of the license, etc.) must be strictly adhered to.

All copyrighted information, such as text and images, retrieved from E-resources or stored, transmitted or maintained with E-resources, must be used in conformance with applicable copyright and other laws. Copied material, used legally, must be properly attributed in conformance with applicable legal and professional standards.

Non-organizational Use

Users may not use E-resources for:

1. Compensated outside work

2. The benefit of organizations not related to the school, except those authorized by a school principal, or the superintendent, for appropriate school-related service.

3. Personal gain or benefit.

4. Political or lobbying activities.

5. Private business or commercial enterprise.

Misuse of E-resources

The school recognizes and allows for the fact that employees and others covered by this policy may, on rare occasions, use the school computer network for non-work or non-school-related purposes. Such use is a privilege and not a right. An example of such use would be the accessing of an information web site on the Internet or sending or responding to an email for necessary personal needs. Such use is to be kept to an absolute minimum and should be limited to breaks or lunch periods. In no way may such use interfere with an employee's work, customer service, responsibilities of the workplace, or the necessary, reputable business of the school. School E-resources may not be used in any way for non-organizational uses as specified in the Non-organizational Use section of this policy. In any and all cases, where acceptable use comes into question, management of the school reserves the right to determine what is appropriate and acceptable and what is not. Violations of school policies will result in one or more of the following actions:

1. User will be notified that the misuse must cease and desist.

2. The project or work will be more carefully supervised.

3. The user will be required to reimburse the school or pay for E-resource(s).
4. The user will be denied access to the E-resource(s), temporarily or permanently.
5. The appropriate school disciplinary action will be initiated. Actions may include sanctions, up to and including, termination of employment or expulsion.
6. Civil action will be initiated.
7. Law enforcement authorities will be contacted to initiate criminal prosecution.

All users are encouraged to report to the Tech Support any suspected violations of school computer policies, such as unauthorized access attempts. Users are expected to cooperate with system administrators during investigations of system abuse. Failure to cooperate may be grounds for disciplinary action.

The school retains final authority to define what constitutes proper use and may prohibit or discipline use the school deems inconsistent with this or other school policies, contracts and standards.

II. E-RESOURCES OPERATION, MAINTENANCE AND OVERSIGHT

Controlling Access to E-resources

User IDs and passwords are the primary method used to authenticate users of Barnstead Elementary’s E-resources. They assist in preventing unauthorized individuals from accessing E-resource systems or particular data stored on systems.

When there is a high threat of password compromise or when an application has particularly sensitive authentication needs, forms of access control other than user IDs and passwords, such as tokens, digital certificates or one-time passwords, can be utilized.

Physical Access Control

Direct physical access to certain E-resources such as servers, data networking devices, and telecommunications switches is restricted.

Rooms containing critical E-resources must be secured strongly. All entrances to such rooms must be closed and locked at all times. Alarms, sensors and other types of physical security systems must be utilized to further secure these facilities and to detect and report emergency conditions that might occur. Signs outside the rooms must not indicate the sensitivity of the equipment inside. Appropriate fire suppression systems must be in place. Equipment should not be left logged on while unattended. Visitors must be escorted at all times.

Authorized personnel may be granted access to server or network equipment rooms through the issuance of ID cards or keys or through the use of passwords or other access codes. These access controls may not be shared with any other personnel. If an authorized person is leaving their current role and should no longer have access to systems, his or her access must be revoked immediately upon the termination of duties. In the case of employees or independent contractors, departments must promptly notify Human Resources of such changes.

All access to server and network equipment rooms made by authorized personnel, escorted visitors, and vendors must be logged when entering the room. Server access logs must be available for review. Vendors must supply the names of all authorized personnel that will be performing on-site work and must keep the list up-to-date at all times.

If school personnel believe that an unauthorized person gained or attempted to gain access to a server or network equipment room, they must contact the school's principal or tech coordinator

E-resources Operation, Maintenance and Administration

All system administrators (those individuals charged with the daily administration of E-resources within a unit of the school) have the following:

Rights

1. Administrative rights over certain E-resources as delegated by the appropriate school officer or unit of the school.
2. Administrative authority to grant other users the authority to read, write, edit, or delete information in files or databases established by them.
3. Administrative authority to establish security controls and protection for information and E-resources under their authority.
4. Employ a variety of security monitoring devices and tools to identify misuse or unauthorized use of systems under their management.
5. To temporarily shut off the school's Internet connection, without prior notice, in order to protect school systems, data and users. A member of ITS management team must give approval for the Internet connection to be shut down.

Responsibilities

1. All system administrators will preserve users' privileges and rights of privacy consistent with this and other applicable school policies.
2. Provide information to users about policies pertaining to use of and access to E-resources.
3. Preserve the availability and integrity of school E-resources, data and systems.
4. Restore the integrity of the affected system in case of abuse, viruses or malfunctions.
5. Determine and authorize the appropriate level of access for each user or class of users.

6. Initiate access change procedures when individual users' circumstances change (e.g., graduation, termination, transfer, leave of absence).
7. Provide or obtain the necessary training for the proper use of E-resources and data made available to users.
8. Ensure that all hardware and software licensing agreements applicable to E-resources are executed by appropriate school authority.
9. Ensure that all server and networking device user IDs are administered in accordance with established policies.
10. Perform monitoring and maintenance of E-resources, and troubleshooting and resolution of technical problems.
11. Assist in the investigation of suspected violations of school policies or procedures.
12. Take reasonable steps to keep log files secure, and physically secure equipment and E-resources.
13. Implement basic logging for all remote access systems and remote access sessions.

School administrators and authorized ITS staff have the following:

Rights

1. To take all reasonable steps necessary to preserve the availability and integrity of E-resources.
2. Reject or destroy email messages and email attachments that are suspected of containing email-borne malicious code, such as viruses and worms.

Responsibilities

1. Protect the security of school E-resources, data and assets.
2. Monitor the usage and content of E-resources in order to administer the systems properly.
3. Maintenance of E-resources and the troubleshooting and resolution of technical problems.
4. Investigate suspected violations of school policies or procedures.
5. Conduct internal audits to evaluate the effectiveness of and compliance with security policies and procedures.
6. Handle any other unusual and compelling circumstances that require system administrator access.
7. Allocate usage of E-resources in accordance with school priorities.

8. Restore the integrity of the affected system in case of abuse, virus or other malfunction.

9. Ensure conformance with legal obligations as they pertain to the administration of E-resources.

Restrictions

1. Access to confidential files and data is allowed only for purposes that fall within the scope of the individuals' role or job responsibilities.

2. Utilizing and obtaining access privileges only to the extent required by the performance of their job responsibilities.

III. POLICY AMENDMENTS

The school reserves the right to change the policies, information, requirements and procedures, announced in this policy, at any time. Changes required by school contractual commitments shall be effective and binding to users upon execution of any such contract by the school. A user shall be deemed to have accepted and be bound by any change in school policies, information, requirements or procedures if such user uses E-resources at any time following announcement or publication of such change.[1]

[1] Acceptable Use of E-Resources Policy. 2007 IT Department, Marquette University,
Milwaulkee, WI. 25 Feb. 2008
< http://www.marquette.edu/its/strategy/aup.shtml>

(Approved: 09/23/08)