



Employee Agreement Technology Acceptable Use Policy

Beacon City School District

1. SCOPE AND DEFINITIONS

The intent of this policy is to make clear the responsible use of the Beacon City School District network and technology systems, not to exhaustively enumerate all possible violations. For purposes of this policy, the district shall consider any of the following subject to the use provisions and limitations defined in this policy:

- file servers, network connections, data lines, infrared nodes.
- desktop computers, printers, laptop units, docking stations, desk or wall data jacks.
- district owned software.
- projection units, electronic white boards, video cameras, televisions, monitors, projection screens, speaker systems and microphones.
- phone / voice systems, including voice mail, wall and desktop handset equipment.
- Library or other security devices including scan devices, cameras, access control modules, keypads, monitors.

2. PROFESSIONAL / EMPLOYEE RESPONSIBILITY: Data, Video and Voice networks have been provided by the “District” as a valuable tool and a necessary component of an employee’s work. In addition, varying work responsibilities result in access to information sources such as software, programs, Internet, district data networks etc. Although employees may have access to these information sources, their use may be restricted and must be specifically authorized. Therefore access and authorization to network or web based district information and technology equipment shall carry a corresponding responsibility within the scope of each employee’s responsibilities to their appropriate use as defined within this policy. District equipment and access is intended for use solely to conduct educational and professional / career development activities. It is the employee’s responsibility to restrict his/her use of said technologies and information resources to these purposes.

3. PRIVILEGES: The use of the electronic information systems is a privilege, not a right. Inappropriate use may result in cancellation of my account, and / or other disciplinary actions tailored to meet the specific concerns related to the violation.

4. ACCEPTABLE/ UNACCEPTABLE USE:

- A. Access rights, employee accounts, and passwords are assigned to individuals only. No employee shall provide others with his/her access privileges or use of district systems using your password. Please be aware that any employee may be held responsible for the actions conducted from or data generated/saved/manipulated within his/her user account.
- B. When using data, video, voice networks, or web information which is owned or operated by other organizations, the employee shall always be responsible for limiting or using said data, video, voice network or web information in accordance with this policy.
- C. Transmission and or use of any material in violation of United States or other states regulations is prohibited. This includes, but is not limited to copyrighted material, threatening or obscene material, or confidential data.
- D. Engaging in commercial activities and/or non educational use of systems, shall be considered a direct violation of this policy.
- E. It is prohibited to access, send or download any of the following: large video/graphics files, pornographic, obscene, profane, lewd, vulgar, rude, inflammatory, threatening materials.
- F. Technology resources are expensive to maintain and operate. It shall be each employee's responsibility to use district systems and supplies judiciously and at all times in accordance with this policy. Wasteful or personal printing, excessive personal file storage, eating / drinking / spilling on equipment, or other actions which compromise the district's equipment, file storage or routine use of supplies is prohibited.
- G. Modifications to hardware, networks or software is prohibited. Additionally employees and or students do not have a right to load software on any district system without the written approval of the Director of Technology.

5. COPYRIGHT:

- A. It is the employee's responsibility to adhere to all copyright laws related to print, data or video use.

6. STUDENT PERSONAL SAFETY:

- A. Employees who supervise students with use and access to "Technology Systems" shall be familiar with the Beacon City School District Student Use Policy Agreement and enforce all its provisions.
- B. All Student "technology systems" use will be supervised by a responsible staff member.
- C. It is the responsibility of the staff member supervising students to maintain a record of equipment use and report immediately any resulting misuse by their students. (know and identify which student is on what computer, or using other technology equipment under their supervision).

7. SYSTEMS SECURITY:

- A. Employees are responsible to insure the security of any district technology equipment, files, information, data, passwords assigned to or created by them.
- B. Employees with access to student records may not use, release, or share these records except as authorized by the Beacon City School District, and /or Federal or State Law.
- C. Once an employee has “signed on” and accessed a district network, he/she shall not leave the workstation unattended at any time.

8. EMPLOYEE LIABILITY:

- A. Employees may be held financially responsible for any unauthorized movement of, or reconfiguration of technology/network resources which results in damage or unnecessary “downtime” to any district data, video or voice system and/or component. It shall be the employee’s responsibility to secure appropriate permission to move, adjust, reconfigure such resources from the Director of Technology, and arrange for assistance from the District Informational Specialists.
- B. Employees assigned “technology equipment” are responsible for its basic care and safety. Excessive wear, damage/repair may result in a financial liability to the employee.
- C. It is the responsibility of the staff member supervising students to maintain a record of equipment use and report immediately any resulting misuse by their students. (know and identify which student is on what computer, or using other technology equipment under their supervision).
- D. It shall be each employee’s responsibility to report any attempts or actions of a person to vandalize, degrade or disrupt technology equipment or system performance.

9. EXPECTATION OF PRIVACY:

- A. Employees shall have no expectation of privacy in files, disks, drives, documents, electronic mail, which has been created in, entered in, stored in, downloaded from, or used on district equipment and systems.
- B. Electronic mail (Pegasus system) has been provided for correspondence and communication as related to your employment in an educational environment and not for personal business use. The district understands that occasional personal communication may occur with family members. However, the district reserves the right to determine when such use is excessive and in violation of this policy.

10. SERVICES AND ASSUMPTION OF RISKS:

- A. The district makes no warranties of any kind, whether express or implied, for services provided and is not responsible for any damages suffered while on the systems, to include loss of data, inaccurate or poor quality information, misdeliveries, service interruptions caused by the system or by your own errors or omissions.
 - B. The district reserves the right to remove files, limit or deny access, and refer staff for other disciplinary actions in accordance with this policy.
 - C. The district reserves all rights to any material (voice, data, video) stored in files, drives or other storage means owned by the Beacon City School District.
 - D. The district and/or network resources are intended for the exclusive use by their registered users. Staff is responsible for the use of his/her account/password and/or access privilege. Any problems which arise from the use of a staff account are solely the responsibility of the account holder.
-

**Beacon City School District
Employee Technology Agreement**

I hereby acknowledge my responsibilities to act in accordance with this Employee Technology Agreement. I understand that if I am found to be in violation of any of the above provisions, it may result in my being subject to disciplinary action, the revoking of my account(s), the collection of equipment / software assigned to me, personal financial liability and / or appropriate legal action.

Name _____
(PRINT)

School/location _____

Signature _____ date _____