BAHRAIN BAYAN SCHOOL

ACCEPTABLE USE POLICY (AUP) 2016-2017

INTRODUCTION

BAHRAIN BAYAN SCHOOL recognizes the importance of technology in providing a relevant and appropriate education. Our goal is to provide students and teachers with access to modern technology in an environment that encourages exploration, individual creativity and educational development.

New avenues of learning that offer unique challenges to the staff and students come with the use of modern technology. The new technologies that use global communication networks provide the students and teachers with learning opportunities that are countless and unmatchable. The power of these systems lies in their ease of use and ability to connect instantly to a growing host of global resources. With every new technology there is the potential for productive use and destructive use. It is the responsibility of the user to use the technology appropriately. The use of the technological facilities provided by Bahrain Bayan School to students and faculty is a privilege.

This Acceptable Use Policy (AUP) is designed to describe how Bahrain Bayan School expects the technology to be used by students, staff, and faculty. Students violating this policy may suffer disciplinary action including but not limited to the loss of privileges relating to the use of technology in the school as described in the Student School Policy. Employee violations of this policy may result in disciplinary actions up to and including probation or dismissal. During the course of the school year, additional rules regarding Internet safety may be added to address emerging technologies. Upon approval by the School Director, any such rules will become part of this Acceptable Use Policy.

Responsibilities of the Technology Department (IT Department)

The Technology Department is responsible for the design, implementation and maintenance of all aspects of the network infrastructure including the management of facilities that connect the school's Intranet to the public Internet. The internal systems that route, switch and interconnect the diverse system within the Intranet at both the hardware and software levels are the specific responsibility of the IT department. Funds to support this mission are included in the IT budget. This includes but is not limited to network support of instructional applications not specifically maintained by vendors outside the BAHRAIN BAYAN SCHOOL (BBS) network. The IT Department supports and maintains the Internet filtering system and all other application servers in its server facility.

Purpose of Educational Mission

BBS provides access to its computer system, including access to the Internet, as a privilege, and not as a right, to its students and staff. BBS has an educational purpose, which includes the use of its system for classroom activities, professional or career development. Users are expected to use Internet access through the computer system to advance educational and personal goals consistent with the mission of BBS and its policies. Uses, which may be acceptable on a user's private personal account on another system, may not be acceptable on a BBS system.

Content that creates a material or substantial disruption to the school will result in student discipline as described in the Student School Policy or staff repercussions up to and including dismissal as described in the Staff School polices.

1. ACCEPTABLE USES

1.1. School computer facilities are for the educational and administrative use of students and staff.

1.2. The purpose of the school's network infrastructure and the Internet is to support and enhance the educational environment of the school.

2. COMMUNICATIONS AND E-MAIL

2.1. Creation or transmission of material in violation of any copyrighted material, threatening or obscene material, or material protected by trade secrets and is applicable to the use of mobile devices. Will result in disciplinary action.

2.2. Student communication with other Internet users is prohibited unless approved by the supervising teacher.

2.3. Student communication with other Internet users is prohibited unless approved by the supervising teacher.

2.4. It is the responsibility of the student user to report to responsible school personnel any knowledge of electronically transmitted attacks made over the Internet or Local Area Network (LAN).

2.5. Employees must not forward confidential or sensitive school emails to a non-school email address that they own or control.

3. NETWORK, PRIVACY, AND SECURITY

3.1. Using the network for any illegal or unauthorized activity, including violation of copyright or contracts, or transmitting any material in violation of any local law is prohibited

3.2. Use for product advertising or for political purposes is prohibited.

3.3. Unauthorized remote access to school facilities via telecommunications facilities is prohibited.

3.4. Using the school's network facilities for financial gain, commercial activity, or any illegal activity is prohibited.

3.5. Any activity that results in the loss of another person's privacy is prohibited. This includes, but is not limited to, copying software or data files containing personal, private, or confidential employee information for the purpose of electronic or physical removal from school grounds.

3.6. Using, viewing, transmitting, or attempting to locate material that is unacceptable in the school setting is prohibited. This includes, but is not limited to, pornographic, obscene, violent, or vulgar images, sounds, music, language, video or other materials not in keeping with the educational mission of BBS.

3.7. Other unacceptable uses of the School's network facilities include:

3.7.1. Unauthorized downloading or installation of software.
3.7.2. Wastefully using resources, such as file space.
3.7.3. Gaining unauthorized access to resources or entities.
3.7.4. Posting material created by another without his or her consent.
3.7.5. Using the computer system while access privileges are suspended or revoked.
3.7.6. Vandalizing the computer system, including destroying data by creating or spreading viruses or by other means.
3.7.7. Intimidating, harassing, or coercing others.
3.7.8. Threatening illegal or immoral acts.
3.7.9. Accessing personal hotspots or other wireless connections not provided by the school.

3.8. Possession or use of hacker utilities designed to circumvent security systems or gain unauthorized access to computer facilities is prohibited.

3.9. IT Resource Monitoring, BBS may install software and/or hardware to monitor and record all IT resources, usage, including email and Web site visits. The school retains the right to record or inspect any and all files stored on or transmitted by school systems.

3.10. Staff members may not disclose sensitive information to persons not authorized to receive it. This includes non-public information such as CPR Numbers, credit card numbers, bank account numbers, health information, or confidential student data. Sensitive hardcopy information must be securely stored according to BBS policies and be destroyed by shredding when no longer needed.

3.11. All employees who have access to or may have access to personally identifiable student records shall adhere to all school standards, and other applicable laws and regulations, as they relate to the release of student information.

3.12. Users shall protect the confidentiality of their password(s) to ensure system security and their own privilege and ability to continue to use the system.

3.13. Abuse or unauthorized use of passwords is prohibited.

3.14. Users who have knowledge of security problems or breaches of security by others are expected to notify a system administrator.

3.15. Any user identified as a security risk for having a history of problems with other computer systems may be denied access to computer facilities.

3.16. Student and staff accounts on software provided by the school are private unpermitted access to other user accounts is strictly prohibited and may result in disciplinary action.

4. CAMPUS COMPUTER FACILITIES

4.1. Staff and students are prohibited from entering restricted areas without permission of the Technology personnel and without supervision. Such areas include, but are not limited to, administrative work areas, server rooms, wiring closets computer labs.

4.2. Removal of equipment from the school premises or relocation of equipment within the school is prohibited unless approved through the o Technology Department. Inventory of equipment, network monitoring, and logging of Internet access are based on network addressing and location within the school.

4.3. Deleting, altering or modifying software residing on school equipment is strictly prohibited. This includes modifying workstation configurations or network security settings.

4.4. Students and staff are expected to use the computer equipment and network infrastructure in the manner provided without alteration.

4.5. Any use of computer facilities which disrupts the educational environment of the school is prohibited.

4.6. Users may be held liable for costs associated with loosing, damaging, or defacing hardware supplied by the school. Hardware refers to the monitor, CPU, keyboard, mouse, printer, and any tech equipment. Computer hardware also includes network infrastructure such as cables, connections, switches, or electrical facilities.

5. INTERNET USAGE AND SITES

5.1. BBS shall prevent access to materials considered to be harmful.

5.2. BAHRAIN BAYAN SCHOOL employs an Internet content filtering by category in meeting the Bahrain government guidelines for Internet safety. Users may encounter material, which students, parents, teachers or administrators may consider to be obscene, inappropriate or offensive. Because of the global nature of the Internet, BBS is not in a position to prevent all unsolicited or unintentional receipt of such materials. Students and staff are expected to refrain from sending, receiving, viewing, or downloading illegal material via the Internet.

5.3. Security profiles are based on individual students and staff members.

6. TECHNOLOGY PROGRAMS

6.1. Programs offered by Bayan School's Technology Department:

6.1.1. iPads Program

6.1.2. Tablet Leasing Program

6.1.3. Bring Your Own Device (BYOD)

6.2. Grade 6 students are automatically enrolled in the Tablet Leasing Program which extends to Grades 7 and 8, an annual fee will be applied. These fees are subject to change.

6.3. Student who receive devices as part of the Tablet Leasing Program must read this agreement and sign attached contract, and get his or her parent to read and sign the contract, and submit it to the technology department.

6.4. The student takes full responsibility for his or her device and keeps it with himself or herself at all times. Devices must be stored and secured in the student's assigned personal locker, or in the designated area as instructed by school when not in use. The school is not responsible for the security of the device.

6.5. The student is responsible for the proper care of the device, and for school devices, they may incur full costs of repair, replacement or any modifications associated with losing, damaging, or defacing device.

6.6. The school reserves the right to inspect a student's device if there is reason to believe that the student has violated the AUP, administrative procedures, and school rules or has engaged in other misconduct while using their personal device.

6.7. Violations of the AUP, administrative procedures or school rules involving a student's personally owned device may result in the loss of use of the device in school and/or disciplinary action.

6.8. The student complies with teachers' request to shut down the computer or closes the screen.

6.9. Personal devices shall be charged prior to bringing it to school and shall be capable of running off its own battery while at school.

6.10. The student may not use devices to record, transmit or post photos or videos of a person or persons on campus. Nor can any images or video recorded at school be transmitted or posted at any time without the express permission of a teacher or the concerned party.

6.11. During school hours the student should only use their device to access classroom related activities.

6.12. The student will not use personal wireless network. Use of 3G & 4G wireless connections is not allowed.

6.13. Students will communicate with faculty exclusively through school email accounts.

6.14. School devices are to be kept away from food and drink any costs resulting from such incidents are to be handled by the user.