Acceptable Use Policy (Staff/Faculty/Students)

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 staff and students come with the use of modern technology. The new technologies that use global communication networks provide the students and teachers with many endless learning opportunities. The power of these systems lie 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.

This Acceptable Use Policy (AUP) is designed to describe how Bahrain Bayan School expects the technology to be used. 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 may be added to address emerging technologies. 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 applications not 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. Other responsibilities include the purchase and management of software and devices.

Purpose of Usage

BBS provides access to its computer system, including access to the Internet, 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 created by any party that creates damaging material or causes substantial disruption to the school's devices, data, or network will result in repercussions by the school including but not limited to discipline, expulsion and possible legal action.

1.1. Acceptable Uses

1.1.1. School computers are for the educational and administrative use of students, staff, and authorized personnel.

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

1.1.3. Students will receive Responsible Use Policies (RUP) depending on their division, that is aligned with the Acceptable Use Policy. The purpose of RUPs is to communicate Educational Technology Rules & Guidelines to students in simplified format.

1.2. Internet Usage and Sites

1.2.1. BAHRAIN BAYAN SCHOOL shall prevent access to materials considered to be harmful.

1.2.2. BAHRAIN BAYAN SCHOOL employs an Internet content filtering by category which meets 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.

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

1.3. Communication and Email

1.3.1. Creation or transmission of material in violation of any copyrighted material, threatening or obscene material, or material protected by trade secrets is prohibited. This is also applicable to the use of mobile devices.

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

1.3.3. It is the responsibility of the user to report to the IT Department any knowledge of electronically transmitted attacks made over the Internet or Local Area Network (LAN).

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

1.4. Network, Privacy, and Security

1.4.1. Network should be used to promote the instructional mission of the school. Users are expected to use it responsibly. The following are considered irresponsible uses of the network and are prohibited:

a. 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.
b. Use for product advertising or for political purposes.
c. Unauthorized remote access to school facilities via telecommunications facilities
d. Using the school's network facilities for financial gain, commercial activity, or any illegal activity.
e. Using VPN or masking software, or using, viewing, transmitting, or attempting to locate material that is unacceptable in the school setting. 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.
f. Unauthorized downloading or installation of software.

g. Wastefully using resources, such as file space, printing, copying, excessive downloading.
h. Posting material created by another without his or her consent.
i. Gaining unauthorized access to resources or entities.
j. Using the computer system while access privileges are suspended or revoked.
k. Intimidating, harassing, or coercing others, or committing threatening illegal or immoral acts.
l. Accessing personal hotspots or other wireless connections not provided by the school during class time.

1.4.2. Unauthorized 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.

1.4.3. Vandalizing the computer system, including destroying data by creating or spreading viruses or by other means.

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

1.4.5. IT Resource Monitoring, BBS may install software and/or hardware to monitor and record facilities, spaces, resources, data usage, including email and Web site visits. IT reserves the right to access any device on it's network at any time.

1.4.6. Users 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.

1.4.7. Users 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.

1.4.8. 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.

1.4.9. Abuse or unauthorized use of passwords is prohibited.

1.4.10. Users who have knowledge of security problems or breaches of security by others are expected to notify the IT Department.

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

1.5. <u>Software and Educational Resources</u>

1.5.1. Powerschool is the main Data Management System used to store students personal and academic information:

1.5.1.1. Divisions are responsible for updating and maintaining accuracy of students' personal information, including but not limited to, contact information, pick up information, parents' names, etc.

1.5.1.2. Private students' records, or records related to mass communication with parents including but not limited to: physical address, email address, etc. are to be changed only through IT department.

1.5.1.3. Any changes in Students' names that do not match passport or nationally issued identification, must be done through the IT department accompanied by parents' request or official documentation to be reflected on the system.

1.5.1.4. Students grades and attendance records (if applicable) can be disabled/hidden through the IT department for a specified time upon official request from the division principal.

1.5.2. Staff members who have access to or may have access to personally identifiable student records shall adhere to all school standards and regulations when sharing information.

1.5.3. Educational Software & Resources used in school, that have not been provided by the IT department must be disclosed to IT, and a copy has to be provided for storage, distribution, and backup.

1.5.4. Software resources for teachers and staff members are to be evaluated, approved, and purchased through the IT department, after primary approval from divisional principals. Divisional principals must submit yearly feedback to support requests for subscription renewals or new requests.

1.5.5. A copy of all media recorded or taken during any school event (e.g., videos, photos, etc.) by a third party (outside the school) must be obtained by PR department, and provided to IT Department for documentation, storage and distribution.

1.5.6. Activation and deactivation of student accounts must be done by the IT Department in accordance with the Finance and Division Principal, activation and deactivation of faculty accounts must be done by the IT department in accordance with the HR and Finance Departments.

1.6. <u>Campus Tech Facilities</u>

1.6.1. 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.

1.6.2. Tampering with or Removal of equipment from the school premises or relocation of equipment within the school is prohibited unless approved through the Technology Department. Inventory of equipment, network monitoring, and logging of Internet access are based on location within the school. Classroom devices such as docking station, smartboard, wireless keyboard mouse are assigned by room and not by teacher, teachers relocating classrooms are limited to moving school laptop and house charger only.

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

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

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

1.6.6. 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, Robotic sets, and any tech equipment. Computer hardware also includes network infrastructure such as cables, connections, switches, or electrical facilities

1.6.7. Robotic lab sets and devices must be used with care, and returned to the appropriate place before vacating the class. Any damage or loss must be reported before leaving the class.

1.6.8. Printers distribution structure within buildings for Faculty usage is executed by the IT Department and decided to ensure efficiency.

1.7. Personal/School Devices

1.7.1. Programs offered by Bayan School's Technology Department:
   1. School-Controlled Devices
   2. Tablet Program
   3. Bring Your Own Device (BYOD)

1.7.2. Students enrolled in the Tablet Leasing Program must use tablets issued by school, no personal devices are accepted.

1.7.3. Teachers and Staff members employed by the school must use school issued devices and school issued accounts for data and email correspondences

1.7.4. Students who bring personal devices to school are recommended to check in their device at the IT Office, as an additional security measure, to avoid device loss within school campus.

1.7.5. 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.

1.7.6. 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 loosing, damaging, or defacing device.

1.7.7. 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.

1.7.8. 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.

1.7.9. The student complies with teachers' request to shut down the computer or close the screen.

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

1.7.11. The student may not use devices to record, transmit or post photos or video 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 person involved.

1.7.12. During school hours students should only use their device to access classroom related activities.

1.7.13. The school wireless network is to be used when on campus.

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

1.7.15. Make sure hands are clean before using school devices.

1.7.16. Keep school devices away from food and drink

1.7.17. Desktops fall under "Campus Tech Facilities" policy, Section 1.4. Laptops fall under "Checked Out Items" policy, section 1.8.

1.7.18. Users are not authorized, and will not attempt, to "fix" or "repair" any school owned hardware or software that may be or appear to be malfunctioning. Malfunctions are to be reported to the IT Department in order to address the issue.

1.8. Checked Out Items

1.8.1. Students enrolled into the Device Leasing Program are given a loaner device when their device is lost or in repair. Student is responsible for the proper care of this loaner device, and ~~for~~ other school devices, they may incur full costs of repair, replacement or any modifications associated with loosing, damaging, or defacing device.

1.8.2. Students can check out devices from the technology department, with below conditions:

1.8.2.1.1. Student must have his/her ID card presented to the IT member upon loaning an item. During class time, the student must have the appropriate pass from his/her teacher/supervisor to check out a device as communicated by the divisional principals.

1.8.2.1.2. Student is to keep his/her phone with the IT department in exchange of a device if he/she is checking the device out during last period prior to a weekend and/or a long school-holiday.

1.8.2.1.3. Students must note down return time and must abide by it. They are only allowed to sign out devices for a maximum of 2 consecutive periods. Students who fail to return their items on time, will have a maximum of 3 warnings according to the following:

- 1st and 2nd warnings:
  - The student will not be allowed to check out any item during the rest of that week.
  - If the device was loaned on Thursday, or before a long holiday, the students will not be allowed to checkout any item during the consecutive week.
- If the student received a 3rd warning, the student will not be allowed to check out any item for the rest of the current semester.

1.8.2.1.4. Students who do not have their ID cards are not allowed to check out any Technology Items.

1.8.3. Users who tamper with devices on purpose, (i.e., remove barcode, tamper with device, etc.) will not be allowed to check out any tech item for the rest of the academic year, and if the School owned device is lost or damaged, user will incur full costs of replacement or repair.

1.8.4. Teachers and staff members can check out technology devices for long or short term periods depending on their use. Long term checked-out items during school year must be returned before leaving for summer break. Items needed over a long break must be checked out from the IT Department.

1.8.5. Users are responsible for the proper care of the loaner device, and for school devices, they may incur full costs of repair, replacement or any modifications associated with losing, damaging, or defacing device.