مدرستنا الثانوية الانجليزية – الفجيرة

OUR OWN ENGLISH HIGH SCHOOL - FUJAIRAH

ACCEPTABLE USE OF TECHNOLOGY FOR STUDENTS

Acceptable Use of Technology - Students

Implemented Date	April 2020
Review Date	February 2021
Next Review Date	September 2021

Purpose

This policy outlines the acceptable use of electronic devices to maintain a safe and secure education environment with the goal of preparing students for the future, improving learning, and fostering digital citizenship.

Definitions

Electronic devices shall include all computing devices that can take photographs, record audio or video data, store, transmit or receive messages or images, provide a wireless connection to the Internet. Examples of these devices include, but shall not be limited to desktops, laptops, tablets and smartphones.

Digital Citizenship is the norms of responsible behavior related to the appropriate use of technology. It encompasses digital literacy, ethics, etiquette, and online safety.

User is any individual granted authorization to use electronic devices. Users may include students, parents, staff, volunteers, visitors, contractors, or individuals employed by Our Own English High School, Fujairah-UAE.

1. Authorized Use of Electronic Devices

Electronic devices brought to school shall be restricted to educational and administrative purposes in approved locations and at times under the supervision of school personnel. Authorized users shall:

1. Use electronic devices in accordance with the expectations set forth in this policy.
2. Comply with guidelines set by school personnel for the use of electronic devices while on school property or while engaged in a school-sponsored activity.
3. Take photographs and audio/video recordings with a consent and when authorized by school personnel for educational purposes.
4. Access the school network using approved infrastructure only.

2. Responsibilities

All users are responsible for:

1. Registering their electronic device with the school and submitting a signed Use of Electronic Devices Agreement prior to connecting with the school network.
2. Ensuring electronic devices are used in accordance with school policies and procedures.
3. Caring, maintaining, securing, and storing electronic devices.
4. Preserving privacy of accounts, login names, passwords, and/or lock codes to maintain security of electronic devices and data.
5. Maintaining safe and productive learning environments when using electronic devices.

Senior Leadership team along with the teachers are responsible for:

a. Informing students of school policy.
b. Establishing and monitoring digital citizenship through the school Code of Conduct and Internet Acceptable Use policy.
c. Responding effectively to disciplinary issues resulting from inappropriate electronic device usage.
d. Communicating appropriately with school personnel, parents, and students if school policy is violated from electronic device usage.
e. Providing information to users explaining how to connect electronic devices to the school network.

2. **Teachers are responsible for:**
    a. Creating equitable learning opportunities that include electronic devices for education purposes when relevant to curriculum and instruction.
    b. Supervising student use of electronic devices.
    c. Responding effectively to disciplinary issues from inappropriate electronic device usage.
    d. Communicating appropriately with administrators, parents, and students if this school policy is violated.
3. **Students are responsible for:**
    a. Using electronic devices for educational purposes in approved locations under the supervision of school personnel only.
    b. Implementing anti-virus and malware scanning on their electronic devices.
    c. Reporting any inappropriate electronic device usage to a teacher or administrator immediately.
    d. Ensuring their electronic devices are charged prior to bringing them to school.
    e. Continuing to learn using an alternative method if an electronic device malfunction.
4. **Parents are responsible for:**
    a. helping their children take all reasonable steps to care, maintain, secure, store, and transport their electronic device.
    b. helping their children preserve the privacy of accounts, login names, passwords, and/or lock codes.
    c. identifying the electronic device by labelling it, recording details such as make, model, and serial number, and/or installing tracking software.
    d. procuring hazard or theft insurance for an electronic device.
    e. encouraging their children to follow school policy and practice digital citizenship.
    f. contacting the school office to communicate with their child during the school day, instead of using text messages, emails, phone calls, or other digital means that have no curriculum related/education purpose.
    g. assuming all responsibility for their child's unauthorized use of non-school Internet connections such as a 3G/4G cellular phone network.

3. Unauthorized Use of Electronic Devices

Prohibited uses of electronic devices includes, but are not limited to:

1. Areas where there is a reasonable expectation of privacy, such as waiting rooms or restrooms.
2. Circumventing school's approved network infrastructure to access Internet connections through Internet Service Provider.
3. Downloading files that are unrelated to educational activities.
4. Engaging in non-educational activities such as playing games, watching videos, using social media, listening to music, texting, or taking personal calls.
5. Using devices to cheat in assignments or tests.
6. Accessing information that is confidential.
7. Using photographs and audio/video recordings for a purpose unrelated to the school assignment.
8. Obtaining unauthorized access and using it to alter, destroy, or removing data.
9. Engaging in cyberbullying which involves using technology to harass, threaten, embarrass, or target another person.
10. Infecting a device with a virus or other program designed to alter, damage, or destroy.
11. Committing a crime under federal, provincial, and/or municipal statues.
12. Infringing upon copyright laws or plagiarizing protected information.
13. Using network resources for commercial or political party purposes.

4. Consequences: Remedial and Disciplinary Action

1. Individuals who do not comply with this Policy will be subject to appropriate consequences consistent with the school Code of Conduct and Internet Acceptable Use Policy.
2. Consequences may include, but are not limited to, the following, either singularly or in combination depending on the individual circumstances below actions to be taken:

    a. Temporary confiscation of device.
    b. Search of device contents to locate evidence of misuse.
    c. Limitations, suspension, and/or revocation of access privileges to personal and school technology resources.

d. Disciplinary measures, up to and including dismissal.
e. Legal action and prosecution by relevant authorities.

Violations may result in disciplinary action up to and including suspension/ expulsion for students.

When applicable, law enforcement agencies may be involved after MOE consultation.

5. Strategies for Unacceptable Use:

1. If students are found taking Pictures / Videos through their electronic devices, the device be confiscated and the matter reported.
2. Any student violating or misusing the Lab computers lab in charge will report to SLT Team for further actions.
3. In distance learning classes students to report online incidents as appropriate.
4. Student's Internet access is regularly monitored for improving the filtering Policy.
5. Computer Labs are monitored by CCTV Cameras.

The use of School technology resource is a privilege, not a right. This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the User Terms and Conditions named in this policy, privileges will be terminated access to the school's technology resources will be denied, BYOD devices will be denied access to the school's network and Wi- facilities and the appropriate disciplinary action shall be applied. The School code of conduct / MOE behavior policy shall be applied to student infractions.

6. Liability

1. Users are solely responsible for the care and use of electronic devices they choose to bring to school. Users bringing these devices to school do so at their own risk.
2. The school and school personnel shall not be liable for the loss, damage, misuse, or theft of any student-owned electronic device: possessed/used during the school day; in/on school buildings, property, vehicles, or contracted vehicles; during transport to/from school, while attending school-sponsored activities.
3. The school and school personnel shall not be responsible for any negative consequences to electronic devices caused by running specific software or by accessing the school network.

7. Technical Support

1. School personnel shall not provide technical support, troubleshooting, or repair for user-owned electronic devices.

8. Cross-reference

This document should be read in conjunction with the following documents also mentioned details below.

1. Online Safety Policy
2. BYOD Policy
3. ICT Firewall Policy
4. MOE Student Behavior Management Policy
5. Password policy

AUP Agreement Form

Please sign below to confirm that you have read and will abide by the acceptable use policy and that you

are aware of the consequences of failure to do so.

I agree to the stipulations set forth in the school Acceptable Use Policy.

Student Name (Please Print):

Student Signature: Date: / /

Student Grade and section:

Parent or Guardian:

As a parent or guardian of this student, I have discussed the standards with my child and understand that misuse of the school's Network, Internet access, Technology Equipment and BYOD scheme will result in the termination of all Internet and Technology privileges for my child and possibly lead to expulsion from the school.

Parent Name (Please Print):

Parent Signature: Date: / /