مدرستنا الثانوية الانجليزية – الفجيرة

OUR OWN ENGLISH HIGH SCHOOL - FUJAIRAH

STAFF ACCEPTABLE USE OF TECHNOLOGY

STAFF ACCEPTABLE ICT USE POLICY

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

Staff Acceptable ICT Use Policy

Introduction

This document sets out the security, administration and internal rules which the staff should observe when communicating electronically or using the ICT facilities provided by Our Own English High School, Fujairah (the 'School'). The Staff should familiarise yourself with the terms of this policy so that you can make a very positive contribution to the use of ICT in the School. This policy applies to all teachers, employees, contractors and visitors of the School.

AIMS AND OBJECTIVES
The Policy

1. Email:

1. Employees must check your school email at least twice a day.
2. Please be aware that email is no more secure than sending a fax or a letter.
3. Email content that may seem harmless to you or even designed to amuse may in fact be seen in a different way by others.
4. If any inappropriate material is received by email, it should be deleted immediately and not forwarded to anyone else.
5. It would be appropriate to discourage the sender from sending further materials of that nature.
6. Comments that are not appropriate in the workplace or school environment will also be inappropriate when sent by email. Email messages can easily be misconstrued. Accordingly, words and attached documents should be carefully chosen and expressed in a clear, professional manner.
7. Think twice before sending an email to large recipients. There may be a more effective way of communicating your request or intention.
8. Official School Email ID should not be used to sign up for any social media, marketing, E-commerce business websites.

2. Monitoring

1. The School's computer network is an educational and business tool to be used primarily for educational and business purposes. You therefore have a responsibility to use these resources in an appropriate, professional, and lawful manner.
2. By default, we must work on trust and assume that all colleagues are using the ICT facilities in a professional manner. The employee should also be aware that the School is able to monitor your use of the Internet, both during school or working

hours and outside of those hours. This includes the sites and content that you visit and the length of time you spend using the Internet.

3. All employees should be aware that external agencies such as the Police may access the email system.
4. Places of work (including educational establishments) have the ability to monitor emails. Emails at our School will not initially be monitored. However, in exceptional circumstances and where there is clear and proven cause for concern, the Management may authorize in writing the examination of contents and usage of email by the School or by a third party on the School's behalf. This could include electronic communications that are sent to you or by you, either internally or externally, to or from the School's email system.

3 Personal Use

1. Employees are permitted to use the Internet and use personal email facilities to send and receive personal messages, provided that such use is kept to a minimum and does not interfere with the performance of your work duties.
2. However, employees should bear in mind that any use of the Internet or email for personal purposes is still subject to the same terms and conditions as otherwise described in this Policy.
3. Excessive or inappropriate use of email or Internet facilities for personal reasons during working hours may lead to disciplinary action.

4 Inappropriate Behavior

Inappropriate Behavior relates to any electronic communication whether email, blogging (e.g. online diaries), text messaging or any other type of posting / uploading to the Internet.
It is commonly recognized that examples of inappropriate behavior are:

- Accessing, uploading, downloading, or distributing indecent, obscene, offensive or threatening material.
- The use of indecent, obscene, offensive, or threatening language
- Engaging in personal, prejudicial, racial or discriminatory attacks.
- Harassing or bullying another person. Harassment is persistently acting in a manner that distresses or annoys another person either by email, online or via texts.
- Knowingly or recklessly sending or posting false, defamatory, or malicious information about a person,
- Using the Internet for gambling or political purposes.
- Accessing material that is profane or obscene, or that encourages illegal acts, violence, or discrimination towards other people.
- Accessing another individual's materials, information, or files without the permission of the person.
- Violating copyright or otherwise using the intellectual property of another individual or organization without permission.
- Using passwords other than one's own without written permission of that person.
- Vandalizing, defined as any unauthorized access and/or malicious attempt to damage computer hardware/software or networks or destroying the data of another user, including creating, uploading, or intentionally introducing viruses.

- Gaining unauthorized access (“hacking”) to resources or entities.
- Downloading and installing VPN’s or using VPN’s to gain access to inappropriate content.
- Altering the set-up of computers as set by the system administrator.
- Using software which is cracked, pirated, or not assigned or approved by ICT Department.
- Seeking to gain or gaining unauthorized access to information resources or other computing devices.

If you mistakenly access such material, please inform the ICT Department immediately. If you are planning any activity which might risk breaking the acceptable use policy (e.g., research into terrorism for a legitimate project) the ICT Department must be informed beforehand.

4.1 Colleagues should familiarize themselves with the relevant UAE legislation covering this topic.

4.2 If a member of staff becomes aware of inappropriate use of the computer facilities by a student, they should report it to the appropriate Head of Section, Supervisor or Line manager.

5.Strategies for Un Acceptable Use:

- User Cannot Install or Remove any software’s in school Laptops / Desktops.
- If anyone trying to attempt / login to network devices ICT team will receive email alerts about wrong credentials login attempt.
- If any users want to access blocked site, if it’s for educational purpose will whitelist the site with the approval from School Principal.
- Any users forget their account password they can self-reset their email account by already verified personal mobile / personal email ID.
- If any device affected by virus or malware attacks will disconnect from network and quarantine to scan the system completely.
- Printers are completely controlled by providing print quota to users, if any users want to print in bulk supervisors to approve the increasing the Print quota request.
- Firewall Filtering is regularly monitored and any blacklist / whitelist with the approval from SLT Team.
- School Website regularly updating with the recent reviewed policies for users to access anytime for most updated version.

6.Privacy

a. In the course of carrying out your duties on behalf of the School, you may have access to, or handle personal information relating to others, including pupils, colleagues, contractors, parents and suppliers. Email should not be used to disclose personal information of another, except with proper authorization.

b. You should ensure that your username and password are not used by anyone else. You must change your password regularly, as per the Password Policy.

c. You are encouraged to either lock your screen or log-out when you leave your desk. This will avoid others gaining unauthorized access to your personal information, the personal information of others and confidential information within the School.

d. Pupil’s information and images must not be stored or distributed on personal email or cloud storage.

7.Distribution and Copyright

a. You should respect copyright. Breaking copyright law occurs when you reproduce a piece of work that is protected by copyright. If you are unsure whether you can use a piece of work, you should request permission from the copyright owner. This includes music files and the copying of CD’s etc. Do not ask the ICT Department to break copyright laws.
b. When distributing information over the School's computer network or to third parties outside the School, you must ensure that you and the School have the right to do so, and that you are not violating the intellectual property rights of any third party.

8.Viruses

a. The Internet is a potential host for computer viruses. The downloading of infected information from the Internet is potentially fatal to the School computer network. A document attached to an incoming email may have an embedded virus.
b. Virus checking is done automatically through virus protection software installed on the network server. If you are concerned about an email attachment or believe that it has not been automatically scanned for viruses, you should contact the ICT Department.
c. If you think that any school computing equipment may have contracted a virus, you must report the matter to a member of the ICT Support Team.

9.Absence

In cases where you are likely to be absent from work for any period of time (including all personal leave and school holidays), you need to make arrangements for your emails to be accessible by the School or ensure that an 'out of office reply' is automatically set. This automatic reply will alert those trying to contact you that you are away from work and that important queries should be directed to a nominated colleague. If you require assistance in installing this feature, please contact the ICT Department. Please ensure that the “out of office” message is disabled immediately on your return to work.

10.Sanctions:

Sanctions can vary depending on the severity of the offence, from a warning or withdrawal of Internet use to suspension or dismissal. Any breach of the law may lead to the involvement of the Police and will be reported to the governing body immediately.

11.General and Best Practice:

1. Think before you print – printing is expensive and consumes resources, which is bad for the environment. If you can use electronic means rather than printing, then do so.
2. Avoid printing very large files.
3. Always log off your computer when you have finished using it.

4. Always back up your work if you are not saving it on the school system. Work saved on the school servers (or "ONE drive") is backed up every night for you, but be careful to save work kept on the desktop or hard drive of your device since these are not automatically backed up.
5. Observe health and safety guidelines – look away from the screen every 10 minutes to rest your eyes and make sure your chair is positioned and adjusted.
6. Housekeep your email regularly by deleting your sent and deleted items.
7. Leave your computer and the surrounding area clean and tidy.
8. If a web page is blocked that you feel you have a legitimate use for please ask the ICT Department and it can be unblocked if approval is given.
9. If you are leaving the school permanently, please ensure you have saved any files or email you want to keep to a memory stick or CD to take home, as these files will be deleted.
10. If in doubt ask a member of the ICT Department
11. Please ensure your students leave the computer rooms clean and tidy with the computers logged off.
12. Extra care must be taken to protect pupil data if stored on portable hard drives and USB sticks. It is considered best practice to avoid storing pupil information on removable devices because of the serious data protection implications of losing said data.
13. Ensure that you follow health & safety guidelines and best practice when students have to use their own devices. This includes ensuring there are no trip hazards from cables. Make sure students take regular screen breaks and that they are sitting at a table with an appropriate chair.

12.Policy Updates

This policy may be updated or revised from time to time. The School will not notify you each time the Policy is changed. If you are unsure whether you are reading the most current version, you should contact the ICT Department.

13.General

The terms and recommended conduct described in this Policy are not intended to be exhaustive, nor do they anticipate every possible use of the School's email and Internet facilities. You are encouraged to act with caution and take into account the underlying principles intended by this Policy. If you feel unsure of the appropriate action relating to use of email or the Internet, you should contact the ICT Department.

14.Cross Reference

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

1. Online Safety Policy
2. Password Policy
3. ICT Firewall Policy
4. ICT Asset Management Policy