HABITAT SCHOOL
AL TALLAH, AJMAN

UNACCEPTABLE USE POLICY

2020-2021

مدرسة هابيتات الخاصة
HABITAT SCHOOL
P.O. Box 8885, Al Tallah, Ajman, United Arab Emirates | Tel : +971 6 731 5353, +971 6 559 3959
E-mail : info@tallah.habitatschool.org | Website : tallah.habitatschool.org

UnAcceptable use policy for IT Systems

Introduction

This Unacceptable Use Policy (UAUP) for IT Systems is designed to protect HABITAT School, our employees, parents and other partners from harm caused by the misuse of our IT systems and our data. Misuse includes both deliberate and inadvertent actions.

The purpose of the policy is to enhance student learning opportunities, promote student achievement, support the professional work of staff, enhance the school's management, information and business administration systems, Provide access to online learning environments.

Scope

This policy covers only internal use of HABITAT School's systems.
Staff members at HABITAT School who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

Unacceptable use

Compromise Their Personal Safety - Send or post detailed personal contact information, images or audio about themselves or other people.

Conduct Illegal Activities - Attempt to gain unauthorised access to any computer system, Install or use software that is not licensed by the school. Make deliberate attempts to destroy data by hacking, spreading computer viruses or by any other means.

Plagiarise or violate copyright laws by -Plagiarising works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.

Access to inappropriate materials -Attempts to access inappropriate material using the schools ICTs are monitored and logged by the school IT department. Some inappropriate material may be filtered or blocked by the school.

Breach Network Security - Providing their password to another person or in response to a request via email (even if it appears as if the email comes from someone they know).

Use Inappropriate Language -Restrictions against 'inappropriate language' apply to public messages, private messages, and material posted on web pages.

Disrespect the Privacy of Others by- Re-posting a message that was sent to them privately, without the permission of the person who sent the message.

<u>Reporting</u>

Students should Disclose to their teacher any messages that they receive that are inappropriate or disturbing .Notify the Class teacher, if they identify a possible security problem or offended by another person's use of ICT.

<u>Consequences of Improper Use</u>

If a student breaches the School's policy, the following consequences may occur:

A letter will be sent to parents informing them of the breach and subsequent sanction. Parents will be required to acknowledge receipt of the letter by returning the acknowledgement slip to the Class Teacher. Sanctions resulting

from breaches could include: A verbal warning, In School Suspension, Police involvement for any illegal activities In the case of serious breaches, parents will be invited to the school to discuss the matter with the Principal .

Duties & Responsibilities

Technical Staff

Ensure that the school's infrastructure is secure and is not open to misuse or malicious attack and that all aspects of the school's ICT systems are secure, in line with the school's guidance and policies.

Teaching staff

They have an up to date awareness of e-safety matters and of current school e-safety policy and practices.
They have read and understood the appropriate agreements.
They report any suspected misuse or problem to the respective supervisor.
Digital communications with students are only on a professional level and carried out using official school systems.
It is understood that social media can play an important part in communication between the school and students, parents however, there is also a need to ensure it is used in an appropriate and safe way.
They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current best practice with regard to these devices

Students

Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
Will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand the Trust's policies on the taking/use of images and on cyber-bullying.
Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety

Policy covers their actions outside of the school gates, if related to their membership of the school.

Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will therefore take every opportunity to help parents understand these issues through communications and the website. Parents will be responsible for: Endorsing the school policy, Accessing the school website in accordance with the relevant Acceptable Use Policy.

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Principal, or nominated representative.

Contacts

If you have any enquiries in relation to this policy, please contact (Principal) who will also act as the contact point for any subject access requests.