MOBILE DEVICE POLICY
AY 2024-25

HABITAT SCHOOL
AL JURF, AJMAN

Creation Date: 20/05/2014

Last Amendment Date: March2024

Next Review Date: April 2025

MOBILE DEVICE POLICY

Purpose & Scope

The purpose of this policy is to define standards for end users who have legitimate business requirements to use a private or School-provided mobile device that can access the School's electronic resources.

This policy applies to, but is not limited to, the use of mobile/cellular phones, laptop/notebook/tablet computers, smartphones and PDAs, and any mobile device capable of storing corporate data and connecting to an unmanaged network, hereinafter referred to as "mobile device."

The goal of this policy is to protect the integrity and confidential data that resides within Habitat's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be compromised. A breach of this type could result in loss of information, damage to critical applications, financial loss, and damage to Habitat's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of Habitat's direct control to backup, store, and otherwise access Habitat data of any type must adhere to Habitat-defined processes for doing so.

Policy

The school has implemented technical solutions to ensure the safe and responsible use of mobile technology for both school-issued and personal devices.

- Access control measures are tailored to meet user requirements, including internet-only access and shared folder network access.
- Broadband performance and capacity have been optimized to support core educational and administrative activities, even with an increased number of connected devices.
- Filtering is enforced on all mobile technologies to regulate internet connections, attempts to bypass these measures are prohibited.
- Clear exit processes are in place for devices no longer in use at school locations or by authorized users. Routine and proactive monitoring ensure adherence to safety protocols.
- Regarding personal devices, users assume full responsibility and liability for any loss or damage resulting from bringing their devices onto school premises. The school does not accept responsibility for lost, stolen, or damaged devices while on school grounds or during school activities, and recommends purchasing insurance for coverage outside the home.
- Users are encouraged to make their devices easily identifiable and to set passcodes or PINs for added security.
- The school is not responsible for day-to-day maintenance or upkeep of personal devices, including charging, software updates, or hardware issues.
- Users are expected to adhere to current Acceptable Use Agreements, including refraining from using personal devices during tests or exams. Visitors receive guidance on permitted mobile technology use per local safeguarding arrangements.

- Users are responsible for keeping their devices up to date with software, security, and app updates.
- Personal devices must be charged before bringing them to school, as charging during the school day is not permitted. Devices must remain in silent mode on school premises and school buses.
- School-provided devices are intended for learning support, and pupils/students are expected to bring devices as required.
- Staff-owned devices should not be used for personal purposes during teaching sessions, except in exceptional circumstances. Printing from personal devices is not supported.
- Confiscation and searching of devices suspected of unauthorized use are within the school's rights.
- Users are prohibited from altering settings that disrupt device functionality.
- School-installed software must remain accessible and in usable condition, with periodic checks to ensure compliance.
- The school ensures that devices contain the necessary apps for school work. School-owned apps remain the property of the school and are inaccessible to students once they leave. Users are reminded to adhere to app age limits and usage terms and conditions.
- Users must obtain permission before photographing individuals and should only take necessary images or videos.
- Devices may be used in lessons under teacher direction**.**

Employees are expected to use good judgment when engaging in personal calls, sending/receiving text messages, and/or Internet usage on their mobile devices during work hours. Excessive personal calls, text messaging, and/or Internet usage during work hours regardless of the phone used can interfere with employee productivity, safety and be distracting to others. Employees who make excessive or inappropriate use of a mobile device may be limited to using such devices only on scheduled break periods.

To protect the privacy of the faculty, staff, students and visitors, employees are prohibited from using their mobile device as a means to photograph and/or record an individual(s) in any form (audio and/or video) without that individual's knowledge and consent.

The use of mobile devices to photograph and/or record confidential information, private information and/or related items is prohibited.

Habitat School will not be liable for the loss of personal mobile devices brought into the workplace.

Any connection to the School's information services must adhere to the Acceptable Use of Technology Policy. Employees may not use any cloud-based apps or backup that allows school-related data to be transferred to unsecure parties.

Certain employees may be issued a school-owned mobile device. Use of these devices is contingent upon continued employment with Habitat School and the device remains the sole property of Habitat School. Excessive use of minutes or bandwidth for non-business activity is discouraged and may result in a Payroll deduction for personal usage.

Upon resignation or termination of employment, the employee may be asked to produce the mobile device and it will be reset to factory defaults using the remote wipe software. Habitat School will not be responsible for the loss or damage of personal applications or data resulting from the remote wipe.

Enforcement

It is the responsibility of the end user to ensure enforcement of the policies above.

This policy is linked with all the other policies of the School