HABITAT SCHOOL
AL TALLAH, AJMAN,UAE

MOBILE TECHNOLOGY POLICY (2022-23)

MEMBERS OF THE COMMITTEE:

MS. MARIYAM NIZAR AHAMED	**PRINCIPAL**
DR. HUMA ATHER	**VICE PRINCIPAL**
MS. THASNI SHAHAL	**SOFTWARE ANALYST**
MR. ABDUL AZEEZ	**SYSTEM ADMINISTRATOR**
MS. NIMISHA CHINNAKUTTAN	**COMPUTER SCIENCE DEPARTMENT**
MS. MOHASEENA USEPH	**COMPUTER SCIENCE DEPARTMENT**

SCHEDULE FOR DEVELOPMENT / MONITORING / REVIEW

The Policy was approved by the Governing body of the school on	01/04/2020
The Implementation of this policy will be monitored by the	Data Protection Team Members
Monitoring will take place at regular intervals	Annually
Review of the policy	Annually
Last Review Date	11/04/2022
Next anticipated Review date	April 2023

MOBILE TECHNOLOGIES

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, smart phones 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 International Indian School'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 International Indian School's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of International Indian School's direct control to backup, store, and otherwise access International Indian School data of any type must adhere to International Indian School - defined processes for doing so.

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational and that this is irrespective of whether the device is school owned/provided or personally owned.. The mobile technologies policy is consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

Policy

- The school allows:

	School / Devices			Personal Devices		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised Device	Pupil / Student owned	Staff owned	Visitor owned
Allowed in school	No	Yes	Yes	No	Yes	Yes
Full network access	No	No	No	No	No	No
Internet only	Yes	Yes	Yes	No	Yes	Yes
No network access				Yes		

- The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices (delete/amend as appropriate):
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. Internet only access, network access allowed, shared folder network access)
- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user.
- *All school devices are subject to routine monitoring*
- *Pro-active monitoring has been implemented to monitor activity*
- *When personal devices are permitted:*
  - *All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access*

- *Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school*
- *The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)*
- *The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues*
- *The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security*
- *The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues*

- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;
- Personal Devices may not be used in tests or exams
- Visitors are provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
- Users are responsible for charging their own devices and for protecting and looking after their devices while in the school
- Personal devices should be charged before being brought to the school as the charging of personal devices is not permitted during the school day
- Devices must be in silent mode on the school site and on school buses
- School devices are provided to support learning. It is expected that pupils/students will bring devices to the school as required.
- Confiscation and searching - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted

- The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
- The school will ensure that devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to students/pupils on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- *Devices may be used in lessons in accordance with teacher direction*
- *Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances*
- *Printing from personal devices will not be possible.*

Employees are expected to use good judgment when engaging in personal calls, sending/receiving text messages, and/or Internet usage on their mobile device 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 item is prohibited. International Indian 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 company-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 International Indian School and the device remains the sole property of International Indian 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. International Indian School will not be responsible for 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 with the policies above.
Based on the severity of violation the following steps will be taken

First violation:-

For Teaching Staff

Verbal warning by Section Head

Name of Section Head (Middle): Ms. Anni . M. Jones

Email ID: sectionheadmid@tallah.habitatschool.org

Name of Section Head (Primary): Ms. Neethu Jomon

Email ID: sectionheadpri@tallah.habitatschool.org

Name of Section Head (KG): Ms Swapna

Email ID: sectionheadkg@tallah.habitatschool.org

For non-teaching staff

Verbal warning by HSE

Name of the HSE officer: Christopher D'Cruze

Email ID: christopherj@tallah.habitatschool.org

Second violation:-

Memo will be issued by the Principal

Name of Principal: Ms. Mariyam Nizar Ahmed

Email ID: principal@tallah.habitatschool.org

Third violation:-

Use of any of school resources for any illegal activity will usually be grounds for summary dismissal, and the school will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

Contact

If you have any queries or concerns regarding this policy, then please contact itsupport@tallah.habitatschool.org.