NAS DUBAI

BYOD (Bring Your Own Device) Policy

Commencing in August 2020, NAS Dubai will allow Students to use their own devices in lessons.

1.Purpose and Reason

The BYOD policy has been designed to ensure that all designated students of the initiative are given the opportunity to develop the necessary skills and literacy to thrive in the digital age.

Student-centered learning is a key value of any 21st Century school and BYOD helps support this philosophy by giving students more opportunities to take responsibility for their own learning and to develop the attributes of the IB Learner Profile.

1.1 What kind of educational activities will the personal devices be used for?

- Working in Microsoft office 365 for various purposes such as producing documents, spreadsheets, and/or slide shows, email communication and collaboration amongst their peers and teachers.
- One Drive and SharePoint for the purpose of collaboration and accessing resources.
- Accessing the NAS online learning environment during class to support learning.
- Access to video and audio recordings to support learning (Only in accordance with the Acceptable User Contract).
- Self-regulation on the use of ManageBac and other key educational platforms
- Accessing Seesaw for teachers to monitor and assess children’s learning

2. Devices and Software

2.1 Suggested Devices

This policy applies to devices which have a screen & physical keyboard permanently attached to it.

Preferred Devices
Secondary Windows Laptop Apple Laptop (MacBook) **Primary** Windows Laptop Apple Laptop (MacBook) Apple iPad with Keyboard

Date: June 2021
Version NO: 5
Creator: GMN
Reviewed By: SLT

2.2 Suggested Minimum System Requirements

Operating System	Windows (Win 10) or MacOS (High Sierra or Higher)
Processor	core i5 ; 1.6GHz or higher
RAM	8Gb Minimum
HDD	128gb Minimum
Battery Life	6hrs Minimum

2.3 Software

- Office 365 must be installed on the device, this is free and comes with the students online Office365 account (login to your 365 account and download office)
- Any other subject specific software that is recommended, is at the responsibility of the user.
- Seesaw class application and Microsoft Office suites to be downloaded for Primary school students

3.Conditions of Use

All BYOD scheme members are required to fill out the AUA policy (Acceptable Use Agreement Policy), signed by both the parent and the student user, with details of make, model & MAC address of device.

3.1 Guidelines for Students

- Students who bring their own device must always adhere to the BYOD policy & AUA policy at all times.
- Each member of the school staff has the discretion to allow and regulate the use of personal devices in the classroom and on specific projects within school.
- Approved devices must be in silent mode while on school campus, unless otherwise allowed by a teacher. Headphones may be used with teacher permission.
- Devices may not be used for non-instructional purposes (such as making personal phone calls and text messaging).
- Devices should be sufficiently charged before the start of school every day.
- Students may not use devices to record, transmit, or post photographic images or video of a person or persons on campus during school hours or during school activities, unless otherwise allowed by a teacher.
- Devices may only be used to access computer files on internet sites which are relevant to the classroom curriculum.
- Students must ensure they have the latest software installed on their devices, relevant to the subject area.

- It is the student's responsibility to maintain sufficient memory capacity on their device to enable its use for educational purpose.

- Devices must have appropriate protection/cases allowing easy carrying of the devices.
- Devices must be clearly labelled, both physically on the device and electronically.
- Devices must have a secure login and password.
- The schools Behavior Policy/Acceptable use policy is applied if students fail to adhere to these guidelines.

3.2 Students, Parents/Guardians and Staff acknowledge that:

- The school's network filters will be applied to a device's connection to the internet and any attempt to bypass the network filters is prohibited.
- NAS Dubai are authorised to collect any device that is suspected of breaching the BYOD policy, the AUC, the data protection and information security policy for the suspected source of an attack or virus infection. If the device is locked or password protected the student concerned will be required to unlock the device at the request of authorised staff with a parent present.
- All students involved in the BYOD program will supply their own devices and be responsible for its safety, whilst on the school premises
- When accessing the school WiFi, they must agree to terms and conditions set out on the online authentication page.
- Students, Staff and Parents/Guardians are prohibited from knowingly bringing a device on premises that infects the network with malware, virus, Trojan, or programme designed to damage, alter, destroy, or provide access to unauthorised data or information.
- Students, Staff and Parents/Guardians are prohibited from processing or accessing information on school property related to "hacking" altering or bypassing network security policies.
- Printing from personal devices will not be possible at school.
- NAS Dubai are not responsible for restoring devices where passwords have been forgotten or the device is locked.
- It is the choice of the individual families to insure devices against loss or damage.
- Personal devices must be charged prior to school and run on battery power while at school.
- NAS Dubai are not responsible or liable for loss or damage of student's personal devices or cases.
- Any student in breach of this BYOD policy will result in the application of the School Behavior Policy, possibly leading to confiscation of the device.
- Online safety is a core element of NAS Dubai's computer science curriculum, where the scope and sequence will be visited numerous times throughout the academic year

- Students should only use Microsoft Teams Chat during lessons for educational purposes and should not create their own teams chat/groups without the involvement of staff
- Students should not accept invitations from any user who is not part of the NAS Dubai community
- Students are not to send any inappropriate messages, images or audio files as per the laws governed by the UAE
- Appropriate use of devices is the joint responsibility of students, staff and parents. Any inappropriate use/behaviour that occurs while outside of school (eg distance learning) should be reported to the school

3.4 Lost, Stolen, or Damaged Devices:

- Each user is responsible for his/her own device and should use it responsibly and appropriately. The School will take no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices.
- IT Service and Computer Science Staff will help users identify how to keep personal devices secure, users will have the final responsibility for securing their personal devices.
- NAS Dubai staff are not responsible for any troubleshooting, repair maintenance or upgrade to any personal device brought into school under the BYOD policy.
- For iPads, we recommend that screen protectors and durable covers are purchased to keep devices safe along with a name tag to distinguish devices
- Personal insurance on devices is highly recommended to ensure accidental damage is covered outside of any potential warranties provided by manufactures. This would be at a personal cost to families

By **opting in**to this communication, you agree with **NAS Dubai Bring Your Own Device Policy** and the above additional guidelines.

If, for whatever reason, you are **not** in agreement with the details contained herewith, **please contact your personal tutor directly**. If we do **not** receive an email indicating that you **do not** wish your child to adhere with the BYOD policy, we will then make direct contact with families.

Date: June 2021
Version NO: 5
Creator: GMN
Reviewed By: SLT