DWIGHT SCHOOL DUBAI

BYOD Handbook

Table of Contents

1.0 Overview

Dwight School Dubai values the role of technology in education and encourages the safe use of personal computing devices in the classroom through our BYOD (Bring Your Own Device) program. This program empowers students to use their personal devices for learning, provided the device meets the minimum specifications outlined in the following sections.

This comprehensive handbook includes the BYOD, Acceptable Use, and Security policies, along with an FAQ section which addresses the common queries. We believe that this program will enhance the learning experience and foster digital literacy among our students.

Parents are expected to read the document and share the signed acknowledgment form with the school's IT Support Team.

1.1 Rationale

We have elected to offer BYOD to allow students to do schoolwork on the platform of their choice. The use of a device students already have promotes sustainability by reducing the environmental impact associated with the production, distribution, and disposal of the additional device provided by the school and furthers the school's commitment to environmental stewardship and sustainability initiatives.

2.0 BYOD Policy

2.1 Purpose

This policy outlines the guidelines and expectations for students, parents, and staff regarding the use of personal computing devices within the school.

2.2 Scope

This policy covers all students in Grades 1 and above.

2.3 Applicability

This policy applies to all personal computing devices brought into the school premises by students and/or connected to the school network.

2.4 Device and Software

Grade 1 to Grade 4:

Students in Grade 1 to Grade 4 should bring an iPad with at least the following specifications

- Screen size of at least 9.7-inches
- Able to run the current version of iPadOS
- Has a protective case/cover

The school's IT department will erase, supervise, and install management profiles on all the iPads (if not already done) before they can be used within the school.

The School IT department will provide full software support, including the installation of all required apps for classroom use. However, device maintenance and hardware issues are the student's or their parent's responsibility. We recommend that parents ensure that their child(ren)'s devices are labeled for easy identification, have an active warranty, and have serial numbers recorded.

Grade 5 to Grade 12:

Students in Grades 5 and above can bring a device that meets the following criteria

- Has a keyboard
- Has an active antivirus software installed
- Has a screen size of at least 13-inches
- Supports LanSchool Air
- Is able to connect to WiFi
- Can be used for a school day without having to recharge

- Supports the current version of Windows or MacOS

Students will be given the necessary help and support to connect their devices to the school wireless network and access the internet. However, device maintenance and other hardware/technical issues are the student's or their parent's responsibility. We recommend that parents ensure that their child's device is labeled for easy identification, has an active warranty, has serial numbers recorded, and, where possible, has location tracking software installed/activated.

Student Laptop screens will be monitored during school hours using Lan School Air classroom management software. Laptops without this software will not be permitted for use in classrooms.

The school may also require the installation of additional applications and/or make configuration changes to the devices as necessary to support teaching and learning objectives.

Such changes will be communicated in advance.

2.5 Responsibilities

Parents:

- Ensure that their child's computing device meets the specifications in the BYOD policy (section 2.4) and it is in good working condition.
- Discuss responsible use of computing devices and digital citizenship with their child.
- Monitor their child's device usage at home and provide guidance as needed.

Teachers:

- Integrate the use of personal computing devices into the classroom activities where appropriate.

- Teach safe use of IT in classroom to students.
- Enforce the school policies and address any violations promptly.

Students:

- Adhere to the school's code of conduct, acceptable use policy(students), Security policy(students), BYOD policy, and other guidelines at all times.
- Use the personal device only for school-related activities while on campus.
- Respect the rights and privacy of others when using your device.
- Be aware that violations of school policies may result in disciplinary action, including but not limited to revocation of access to IT services within the school and/or the removal of school place.

IT Department:

- Ensure that all students are able to connect to the school wireless network.
- Provide appropriate access to the school's IT resources, including apps required for classroom activities and exams.
- Provide support where applicable.
- Enforce the school's IT policies and procedures.

3.0 Acceptable Use Policy

3.1 Purpose

This policy outlines the acceptable use of IT resources for students within Dwight School Dubai.

3.2 Scope

This policy covers all enrolled students.

3.3 Applicability

This policy applies to all computing devices used by students, including personal devices.

Students should use Dwight IT resources only for the purpose of teaching and learning within and outside the school premises.

Prior permission should be sought from the IT department or Head of School for exceptions.

All students are prohibited from using Dwight IT resources in a manner that violates local laws or other school policies or potentially affects network services. Examples of unacceptable use include but not limited to:

- Any activity that violates local laws.
- Any activity that violates other school policies.
- Any activity that leads to damage of equipment, software, or data that belongs to others.
- Any activity that violates the privacy of other users.
- Any activity that violates copyright or intellectual property rights.
- Any attempt to circumvent/bypass security controls put in place by Dwight IT Department.
- Installing or spreading malware on the network.
- Any activity that disrupts teaching and learning.
- Any form of cyberbullying or harassment.
- Posting or circulating content with hate speech, discriminatory language, or promoting violence and illegal activity.
- Using the school IT resources for personal use.
- Any posts/publications that harm the School's image or reputation
- Unauthorized use of accounts, passwords, PINs of others.
- Unauthorized use of computing devices that belong to others.

These are just examples of prohibited actions and are not exhaustive. Any student in doubt about acceptable activity should contact the IT department for clarification.

3.4 Enforcement

Violation of this policy will result in the loss of network access privilege and/or disciplinary action up to and including removal of the school place.

4.0 Security Policy

4.1 Purpose

This policy outlines the security requirements for student computing devices, accounts, and network security restrictions.

4.2 Scope

This policy covers all enrolled students.

4.3 Applicability

This policy applies to all computing devices used by students, including personal devices and all accounts provided by the school.

4.4 Device Security

Device security for iPads are managed and enforced by the school's IT department using Mobile Device Management. Restrictions may include reduced functionality of the device and restricted availability of apps during school hours.

Any device that isn't an iPad must have endpoint security software (with an active subscription/license) installed. The school may require the students to install an app and/or make a configuration change to their devices to assess the security posture of the device before they can connect to the school network. All

devices must have a password/PIN/biometric (where available) lock set.

The school takes all reasonable measures to safeguard its network, devices, and internal systems, including data residing in school-managed cloud servers. The school will not be responsible for security events, ransomware, or malware on personal devices connected to the school network.

4.5 Account Security

Students are required to create secure PIN code or passphrase that meet the minimum complexity requirements for their device, network and cloud accounts. Multifactor authentication should be enabled wherever possible. Students should keep their account credentials private and not share them with others, as they will be held liable for any activity originating from their account.

Any suspected account compromise or loss of access should be reported to the school's IT department or the Homeroom teacher immediately.

4.6 Email Security

All students from G1 and above are issued a school mailbox. Mailboxes for G1 and G5 can only communicate with other Dwight Dubai mailboxes; they cannot communicate with external email addresses.

The email account should only be used for official school-related services and communications. Email content should adhere to the school's code of conduct and acceptable use policy, refraining from inappropriate or offensive language. Sending "spam," chain letters, or any other type of widespread unauthorized distribution of unsolicited mail is prohibited.

All email communications are logged and monitored. The school, at its discretion, can choose to audit/inspect student mailboxes at any time.

The school has security policies in place and takes all reasonable measures to prevent malicious or unwanted emails from reaching the students' mailboxes. Students should still exercise caution when opening email attachments or clicking links from unknown or suspicious sources. Any suspected malicious email should be reported to the school's IT Department.

4.7 Network Security

There is no expectation of privacy when connected to the school's network; all network traffic is monitored and logged. Student are liable for any traffic generated from their devices. Network bandwidth is a shared, finite resource, both within the School and in connecting to the Internet. Students must make reasonable efforts to use this resource in ways that do not negatively affect others in the network.

Students who choose to store or transmit personal information such as credit card numbers, or certificates or use Internet "wallets" do so at their own risk. The school is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property.

The school has network security policies in place to protect students and secure devices connected to the school network. Any attempt to bypass these policies, including the use of 3G/4G/5G mobile connections or VPN, is prohibited.

4.8 Enforcement

Violation of this policy will result in the loss of network access privilege and/or disciplinary action up to and including removal of the school place.

5.0 FAQs

5.1 PREK, KG 1 and KG 2

1) What is the device policy for PreK, KG1 and KG2?

The school will issue a device (iPad or similar) from the shared resource pool to use in the classroom. Parents are not required to procure a device.

5.2 Grade 1 to Grade 4

1) What is the device policy for Grades 1 to 4?

Students are required to bring an iPad meeting the recommended specs (section 2.4). These devices will be supervised and managed by the School's IT Team.

2) Where can I buy a new iPad?

You can use our partner's portal to procure a device:

https://eshop.allprints.ae/collections/dwight-school-dubai

If prompted for a password, please use: DSD2024

Devices procured through our partner carry additional discounts and bundled offers. In addition, these devices will be pre-enrolled to the school management system, making them ready to use out of the box.

Alternatively, parents can also choose to procure their device from any Apple-authorized resellers.

The school will not be responsible for any issues related to payment, logistics, warranty, etc., for the devices, including those procured through the partner portals.

3) I already have an iPad – Can I use it?

You can use the device if it meets the recommended specs (section 2.4). Devices procured outside the school partner's portal require supervision. You need to book an appointment (the booking link will be shared separately) with the IT Team for device supervision before being allowed to use it in the classroom.

4) What is iPad supervision?

Supervision gives schools greater control over the devices. With supervision, the IT administrator can apply extra restrictions like turning off AirDrop or preventing access to the App Store. It also provides additional device configurations and features, like silently updating apps or filtering web usage.

For devices procured outside the school partner's portal, the IT administrator needs to completely erase your device to set up supervision.

5) Do I need to bring my iPad for supervision?

Supervision is only required for devices procured outside the school partner's portal. You need to book an appointment (the booking link will be shared separately) with the IT Team for device supervision before being allowed to use it in the classroom.

6) I am an existing student who was issued an iPad when I joined the school –

6.1) Can I continue using it at School?

Yes, you can continue using the device.

6.2) Do I need to bring the device for supervision?

No, they are already supervised.

6.3) How can I fix my school iPad if it is damaged?

The school IT Team can facilitate service requests on behalf of the parents provided the device has an active warranty.

6.4) My school iPad is broken. Can we purchase a new one?

Yes, please refer to point 2.

7) What support will be provided by the school for the devices?

The school IT Team will provide full software support (OS and app installation/updates, connectivity, restrictions, etc.) for your devices.

Hardware support is not provided – parents should work with the reseller/OEM directly for hardware-related issues.

8) Will I get a loan device if my device is out for service?

Depending on availability, the school may allocate a loan device for use in the classroom. Loan periods cannot exceed more than two weeks, and the students must return the devices to the IT office at the end of the school day.

Parents can also send another device to the school during this time. Unsupervised devices are permitted upon approval by the Teacher/Director of IT and for a period not exceeding two weeks from the first connection.

9) My iPad is missing, can you find it for me?

The IT Department can assist by enabling "Lost mode" on supervised iPads and locate them provided the device has sufficient charge and is connected to a known wireless network. The school will not be liable for missing devices (both within and outside the campus).

10) What happens when I leave the school?

You can contact the IT Team (servicedesk@dwight.ae) and request to release the device from the school management system. It may take up to 2 business days to complete the

request; you will receive a confirmation email from the IT Team when the release is complete.

5.3 Grade 5 to Grade 12

1) What is the device policy for Grades 5 to 12?

Students are required to bring a laptop meeting the recommended specs (section 2.4). The school will provide access to the Internet for devices that meet the recommended specs and have the mandated software (section 2.4).

The school IT Team will ensure the necessary policies and tools are in place to monitor the device's internet usage at school and will also implement the required controls to safeguard the school's IT infrastructure and its devices.

2) Where can I buy a new Laptop?

You can use our partner's portal to procure Apple Macbooks:

https://eshop.allprints.ae/collections/dwight-school-dubai

If prompted for a password, please use: DSD2024

Alternatively, parents can also choose to procure their devices from any resellers.

The school will not be responsible for any issues related to payment, logistics, warranty, etc., for the devices, including those procured through the partner portals.

3) I already have a laptop – Can I use it?

You can use the device if it meets the recommended specs and has the mandated software mentioned in section 2.4.

4) What is LanSchool Air, and which devices support it?

LanSchool Air is a classroom management software that keeps students safe and engaged while learning with real-time oversight and

digital guardrails. Devices running on the latest Windows or MacOS can support LanSchool Air.

5) I am an existing student who was issued a laptop when I joined the school –

5.1) Can I continue using it at School?

Yes, you can continue using the device.

5.2) What changes will apply to my device post-BYOD implementation?

Your device will be gradually released from the school management system. The school IT team will get in touch with the student and their parents to inform them about the device management transition process and to hand over the device administrator credentials.

5.3) How can I fix my school laptop if it is damaged?

The school IT Team can facilitate service requests on behalf of the parents provided the device has an active warranty. The school IT Team can also arrange quotations for out-of-warranty repairs upon parent request.

5.4) My school laptop is broken. Can we purchase a new one?

Yes, please refer to point 2 in this section.

6) What support will be provided by the school for the devices?

The school will provide support to connect the device to the internet, provide access to apps needed for classroom activities/exams and with any minor issues that may crop up. The school will not be responsible for device maintenance, updates, crashes, and other major OS issues.

Hardware support is not provided – parents should work with the reseller/OEM directly for hardware-related issues.

7) Will I get a loan device if my device is out for service?

Depending on availability, the school may allocate a loan device for use in the classroom. Loan periods cannot exceed more than two weeks, and the students must return the devices to the IT office at the end of the school day.

Parents can also send another device to the school during this time. Please note the school will only provide access to the Internet for devices that meet the recommended specs (section 2.4).

8) My device is missing, can you find it for me?

It is the responsibility of the student to secure the device while in school. Any missing devices should be reported to the reception immediately. Our security team will make reasonable efforts to find out if the device is still in the school. The school will not be liable for the device if it cannot be found.

9) What happens when I leave the school?

No change is required as the devices are not managed. However, we recommend backing up your files from the school cloud services (Google Workspace, Adobe Cloud, Microsoft 365, etc) if you need copies of your work.

Acknowledgement Form - BYOD

I acknowledge that I've read and agree to the following school policies and procedures mentioned the handbook.

☐ BYOD Policy
☐ Acceptable Use policy
☐ Security Policy

Student Details	
Pupil Name	
Pupil ID	
Parent Name	**Signature**

Notes:

- The iSAMS Parent Portal contains the latest version of the policies. Policy changes will be communicated via email. You don't need to fill out the Acknowledgement Form again for subsequent policy changes. The school will assume that you have accepted the changes in the policies unless the School receives a written objection.

- Students will be informed about these policies by the advisors during their homeroom and will arrange for the required training sessions. They are required to sign the Acceptable Use Agreement for records following the training session.

IT Use Only			
Device Model		Serial Number	
Mac address		SDP Tckt No.	
IT Engineer		**Signature**	