DUBAI GEM PRIVATE SCHOOL

STRIVE FOR EXCELLENCE

FAQ – BRING YOUR OWN DEVICE (BYOD)

GOING PAPERLESS

In an effort to increase access to 21st Century skills and go paperless, DGPS mandates the use of personal devices **such as laptops/tablets/Ipads**. Students will be expected to comply with all class and school rules while using personal devices.

1. **Do students have to register their devices?**
   Yes, students will have to register their devices with the DGPS IT Department. Please note that parents and students will need to sign the DGPS Acceptable Use Agreement prior to the device being registered to the DGPS network.

2. **When can students use devices?**
   Students can use the devices only under teacher's supervision.

3. **Are students allowed to access social networks?**
   No, students will not be allowed access to social media using school network during school hours. The school will disable access to all the social network applications.

4. **Can we protect our network and student devices from malware and unauthorized content?**

- We have secure WIFI coverage throughout the school. In addition, students are taught about digital citizenship and staying safe online.
- We have Sonicwall security system to secure our school computers and servers from malware & to block unauthorised content, but for student owned devices we do not have any control on malware or unauthorized content. If the student device is loaded with any kind of Hotspot shield or VPN, then the student device will have access to all kinds of unauthorized content that will lead to malware attack.
- The school is not responsible for the security of student devices.

5. **Do you have anti-virus, URL filtering, secure remote access, and data protection in place?**
   The different kind of tools for the above are:

- **McAfee Enterprise -** Antivirus tools which are installed on all the school computers and Servers guaranteed to detect or delete the malware, Trojans from the computer.
- **Sonicwall Secure VPN Access –** Access to the school network from any other network is given only to the management and IT staff.

- **Veeam One -** To protect the data on the server, server data is backed up every day onto our data store.
- **Manual Backup -** To protect the data, even if our data store fails due to hardware or software failure, manual backup is taken twice a week during school working days.
- **Sonicwall CFS -** Controls URL filtering only on school computers and servers. However, we cannot intercept and control any connectivity done through Hotspot or Tethering or using personal 3G/4G data packages.

6. **Who is allowed to get on the network?**
   During school hours & in the school premises, only devices that are registered with the school IT department can access the network.

7. **Will you allow off-campus access to the school network?**
   No.

8. **Are mobile phones allowed as a substitute to a device?**
   No, under no circumstance will mobile phones be allowed as a substitute during lessons. All students must carry their personal devices.

9. **What are the main Learning Platforms used by the school?**
   Google classroom, Google Meet, Microsoft Teams, Seesaw (FS & KS1) & Zoom.

10. **Where will students charge their devices?**
    Students should ensure that their devices are fully charged at the start of the school day. All classrooms are equipped with charging stations, which can be used in case the device runs out of charge.

11. **How will devices be secured when not in use?**

Student Device Care and Security

It is important that students take responsibility for their own equipment, naming their device, handling it carefully and storing it securely when not in use.

Care and Security of Personal Devices

Mishandling portable devices is the largest cause of problems. Most devices will come with care guidelines which we advise users to read. The following are conditions that we recommend:

- Students are responsible for their own devices. The school will not be responsible for any damages or loss of devices.
- Students should always turn off and secure the mobile device and BYOD devices after they are done working to protect their work and information.
- Adhering to general school rules concerning behaviour and communication that apply to Technology equipment use.
- Portable devices should be protected by a username and password. This should not be disclosed to other students.
- Always store the portable devices in the protective bag. Avoid storing it at the bottom of the school bag – Pressure on the portable device can cause permanent damage to the screen and other components
- Do not store anything additional to the portable devices within the case /sleeve (e.g. cords, papers or disks), as this may damage the screen.
- Never lift the portable device by the screen. This will stress the hinge mechanism, which also carries the power supply to the screen.
- Never leave portable devices in a car or in an exposed area where it can be stolen.
- Never leave devices in unsupervised areas during the school day.
- Using computers/mobile devices in a responsible and ethical manner.

12.Do you have a plan for loaning equipment to students without a device?

No, DGPS has no provision for loaning devices to students.

13.What are the policies and procedures for Lost, Stolen, or Damaged Devices?

Each user is responsible for his/her own device and should use it responsibly and appropriately. Dubai Gem Private School takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. While school employees will help students identify how to keep personal devices secure, students will have the final responsibility for securing their personal devices.

14.Will the school provide technical support for the students' devices?

DGPS does not guarantee connectivity or the quality of the connection with personal devices. Dubai Gem IT department is not responsible for maintaining or troubleshooting student devices however limited support will be provided on a best effort basis.

15.What are the consequences in case of violation of DGPS BYOD policy?

- The use of BYOD is a privilege, not a right. This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of

technology resources. If a person violates any of the User Terms and Conditions named in this policy, privileges will be terminated, access to the school's technology resources will be denied, BYOD devices will be denied access to the school's network and Wi-Fi facilities and the appropriate disciplinary action shall be applied. The School code of conduct / behaviour policy shall be applied to student infractions.

- Violations may result in disciplinary action up to and including suspension/ expulsion for students. When applicable, law enforcement agencies may be involved after KHDA/MOE consultation.

16. What types/models of devices can be brought?

The device must be internet capable and have the ability to create and edit common documents such as word-processed documents, spreadsheets and presentations. It should also have the ability to read ebooks and pdfs. To this end, we would allow netbooks, a laptop or a tablet of 7 inch screen size or larger. If parents and students are considering purchase of devices we have produced some guidelines to assist in this process- **Please check the guidelines in Appendix A.**

APPENDIX A

GUIDELINES

Laptop Specification:

2022 Apple MAC Book Pro Processor : Apple M2 chip with 10-Core CPU Hard Drive : 256 GB SSD RAM : 8 GB Display Size : 13 Inch OS : MAC OS Price Range : 4700 to 4900 AED	**Apple MAC Book Air – M1** Processor : Apple M1 with 7-core GPU Hard Drive : 256 GB SSD RAM : 8 GB Display Size : 13 Inch OS : MAC OS Price Range : 3500 to 3700 AED
Lenovo – IdeaPad Processor : Intel I5 Core 11th Gen Hard Drive : 256 GB SSD RAM : 8 GB Display Size : 15.6 Inch OS : Windows 10 or 11 Antivirus: Kaspersky Internet Security. Price Range: 1700 To 1900 AED.	**Dell – Inspiron Series** Processor : Intel I5 Core 11th Gen Hard Drive : 500 GB SSD RAM : 8 GB Display Size : 15.6 Inch OS : Windows 10 or 11. Antivirus : Kaspersky Internet Security. Price Range : 2500 To 3000 AED
HP – 250 G8 Processor : Intel I5 Core 11th Gen Hard Drive : 256 GB SSD RAM : 8 GB Display Size : 15.6 Inch OS : Windows 10 or 11. Antivirus : Kaspersky Internet Security. Price Range : 1500 To 1700 AED	

Tablet Specification:

Apple - IPAD AIR (4th Gen) Brand : Apple Processor : Apple A14 Bionic CPU Speed : 3 GHz RAM : 4 GB Storage : 64 GB Internal Display : Retina display 10.9 Inch OS : IOS 14 Price Range : 1600 to 1800 AED	**iPad 9th Generation** Brand : Apple Processor : Apple A13 Bionic CPU Speed : 2.65 GHz RAM : 3 GB Storage : 64 GB Internal Display : Retina display 10.2 Inch OS : IOS 15 Price Range : 1200 to 1500 AED
Samsung Galaxy Tab S7 FE Brand : Samsung Processor : Qualcomm Snapdragon 750G RAM : 4 GB Storage : 64 GB Display : 12.4 Inch OS : Android Price Range : 1400 to 1800 AED	**Lenovo Chromebook Duet** Brand : Lenovo Processor : MediaTek Helio P60T RAM : 4 GB Storage : 128 GB Display : 10.1 Inch OS : Chrome OS Price Range : 900 To 1200 AED

Reviewed: September 2022