مدرسة التفاحة العالمية
The Apple International School

Bring Your Own Device (BYOD) Policy 2024-25

- ***This procedure is reviewed annually to ensure compliance with current regulations.***
- ***This policy applies to the whole school including SMT & Governors.***
- ***The Apple International School is committed to safeguarding and promoting the welfare of our students, staff, and fraternity.***

Ref No.: AIS / BYOD / 01 / 2024-25	Policy: **Bring Your Own Device Policy**
Approved by: **Principal**	
Reviewed by: 1) School Principal 2) Vice Principals 3) Senior Manager QA & School Welfare	Implemented by: **IT Department**
Reviewed Date: **Feb 2024**	Next Review Date: **Feb 2025**

TABLE OF CONTENTS

1.0 - Purpose 3
2.0 - Scope 3
3.0 - Objective 3
4.0 - Program Inclusion and Student Registration Process 3
5. Device Specifications 4
6. Educational Use and Benefits 5
7. Device Safety, Security and Maintenance 5
8. Digital Governance and Compliance Committee 6
9. Acceptable use of Technology Guidelines 7
10. Student's Roles, Responsibilities and , and Guidelines 9
11. Responsibilities of Parent / Guardian 11
12. Responsibilities of School 12
13. Compliance with Laws 13
14. BYOD Technical Support 14
15. Promotion of the Policy 14
16. Policy Review 15
17. Conclusion 15

1.0 - Purpose

The BYOD policy at Apple International School allows students to bring and use their personal devices for educational purposes within the school, under the guidance of their teachers. The policy aims to enhance learning experience and foster 21st-century skills by providing access to online resources and tools that support the integration of technology into the curriculum allowing educators to design more engaging and interactive learning opportunities.

2.0 - Scope

This policy outlines the terms and expectations for all students at Apple International School who use their own devices, such as tablets or laptops, for educational purposes. The policy outlines the acceptable use of personal devices, the school's Wi-Fi network, computer/digital systems, and electronic communications. The policy aims to promote responsible and safe use of technology for teaching and learning purposes. It also protects all users from cyberbullying and guides them to recognize and address it appropriately.

3.0 - Objective

The BYOD policy aims to enhance learning and promote ethical and responsible technology use. It allows students to use their own devices to access online resources, tools, and content that support the curriculum. It also establishes guidelines and expectations for device usage, such as teacher approval, Wi-Fi and digital system respect, cyberbullying prevention, and security and maintenance awareness. The policy's goal is to ensure a secure and conducive digital learning environment for all students.

4.0 - Program Inclusion and Student Registration Process

The BYOD program at Apple International School is designed for students from Year 1 and upwards, recognizing that different classes may have varying device requirements to align with their academic needs and objectives.

The device requirements for each class are as follows:

Year 1 – 10	• Device Type: iPad or Android/Windows tablets (or a similar tablet device). • Exclusion: Any mobile phones including Smartphones and smart watches are not permitted (However if the students are self-walkers they needs to get the permission from respective section head and proceed accordingly). In case if the phone is found misused it will be confiscated and will be given only at the end of the Term only to parents.) Devices must not have eSIM/SIM cards installed. • Rationale: Aligned with the curriculum and software requirements for the specified grades.

Year 11 -13	• **Device Options:** iPad, Android/Windows tablets, or Laptop. • **Exclusion:** Smartphones and smart watches are not permitted. Devices must not have eSIM/SIM cards installed. • **Rationale:** To prepare students for the challenges of secondary school and future academic endeavors.

Registration process as follows:

1. The IT team will handle the registration of devices for each student.
2. Only devices registered by the IT team will be granted access to the school network.
3. Registered devices will be authorized to connect to the school network, ensuring a secure and controlled digital environment.
4. Students are strongly advised to bring the same registered device to school consistently.
5. Consistency helps prevent disruptions and ensures a seamless learning experience.
6. Students can log in to the school network using the credentials provided by the IT department.
7. Login information will be securely managed to protect student data.
8. Students must install Office 365 applications (Word, Excel, PowerPoint, Teams) on their devices using the school-provided Office 365 account. The IT department will guide the installation process, offering support as needed. Regular updates are encouraged to access the latest features, ensuring a seamless and productive learning experience.

5. Device Specifications

The device specifications are as follows:

The BYOD policy includes a range of devices, including iPad or Android/Windows tablets and laptops. The specific devices permitted within the school are determined by the IT Administrator.

iPad/Tablets:

Screen Size	10”-13” preferred; Any iPad or Android/Windows tablets.
Storage	64 GB minimum (128GB preferred).
RAM	4GB minimum (8GB preferred).
Battery Life	4 hours or more.
Wi-Fi	Wi-Fi capable 2.4/5GHz supported (802.11a/b/g/n)
Operating System	iOS version 10.0 or later. Android operating system version 7 or later
Accessories	Protective bag/case. Headphones during external exams.

Laptops:

Screen Size	13” preferred
Processor	Intel® or AMD processor with 64-bit support 8th Gen Intel Core i5; 2 GHz or faster processor Or equivalent such as the new M1 chips from Apple
Storage	128GB minimum
RAM	4GB minimum (8GB preferred).
Battery Life	4 hours or more.
Wi-Fi	Wi-Fi capable 2.4/5GHz supported (802.11a/b/g/n)
Operating System	Windows 10 or later. MacOS 10.14 or above
Accessories	Protective bag/case. Headphones during external exams.

We encourage parents to organize the use of a recent model device as these devices will ensure compatibility and supportability for a longer period. However, this is not a requirement of the program, and if students only have access to an older model, then the school will allow its use.

6. Educational Use and Benefits

The BYOD program at Apple International School allows students to access various educational purposes at school. Some of the benefits of this program are:

1. Students can access a variety of online resources and tools that support their learning and development of 21st-century skills.
2. Students can participate in international benchmark tests that are conducted online by ministry approved agencies in Dubai, such as CAT4, e-TIMSS, e-PISA, e-PIRLS, PASSME, GL PT, and NGRT. These tests are part of the holistic educational experience offered by the BYOD policy.
3. Educators can leverage technology to create interactive and engaging learning experiences for students, integrating digital content, assessments, and activities into their curriculum. The program reflects the school's vision of being a leader in educational innovation.

7. Device Safety, Security and Maintenance

Students who choose to bring their own devices to school must be aware that the school does not assume any liability for the security, maintenance, or repair of these devices. Students are solely responsible for taking care of their devices and are expected to adhere to the standards outlined below:

1. **Security**: Students must use strong passwords for their devices and user accounts and protect them from unauthorized access. Passwords must have at least eight characters, with a mix of uppercase and lowercase letters, numbers, and symbols.

2. **Confidentiality**: Students must not share their passwords with anyone and must change them regularly to prevent hacking or misuse. Students must also respect the privacy and intellectual property rights of others, and not access, copy, or distribute any unauthorized or inappropriate content.
3. **Compliance**: Students must follow the school rules and regulations regarding the use of devices in class, during exams, and on school premises. Students must also comply with the acceptable use policy of the network and online platforms, and not engage in any illegal, unethical, or disruptive activities.
4. **Maintenance**: The school is not responsible for the security, maintenance, or repair of personal devices. Students are expected to take reasonable precautions to safeguard their devices.
5. **Accidental Damage and Theft**: The school does not provide accidental damage or theft cover for student-owned devices. Liability is limited unless the device is under the direct supervision of a staff member.
6. **Technical Support**: The school is committed to providing limited technical support, as detailed in Section 14 of this policy. This support aims to assist students and parents with any device- related inquiries or challenges within the defined scope.

8. Digital Governance and Compliance Committee

The DGCC committee oversees the implementation and compliance of the BYOD policy. The committee is composed of key stakeholders, such as the Principal, Vice Principal, Head of Secondary, Head of Primary, MSO, designated ICT personnel and the IT Administrator, who manages policy and practice regarding all aspects of online safety and digital platforms.

The BYOD program is a collaborative effort between the staff and the committee, who are responsible for ensuring its effective and safe implementation in the school. They act as role models and teachers, demonstrating how to use personal devices for learning purposes, in accordance with the curriculum and the school's Wi-Fi Network and computer/digital system.

The committee ensures that all staff and students receive comprehensive training on the BYOD policy, cyber safety, and ethical technology use. Moreover, the committee organizes awareness programs for students and parents to encourage responsible device usage.

The DGCC committee at APPLE INTERNATIONAL SCHOOL has these responsibilities:

1. Each committee member is required to sign, confirming their understanding of both the BYOD Policy and the Acceptable Use Policy (AUP) within the school.
2. Attending and leading training sessions on digital safety and policy changes
3. Implementing and enforcing the BYOD Policy within the school.
4. Educating staff and students to model responsible digital usage, integrate personal devices into the curriculum, and educate students on acceptable and safe Internet use.
5. Raising awareness and preventing cyberbullying among students and staff, provide guidelines on how to recognize and address it, and creating a safe digital environment for all users.
6. Communicating and collaborating with staff on digital resources and promote the benefits and risks of using social media responsibly.
7. Contribute to policy enforcement, reporting any policy violations, and recommending necessary updates during policy reviews.

The DGCC committee and the entire school community work together to create a positive and secure technological environment, ensuring that digital tools enhance the learning experience while maintaining safety and ethical standards.

9. Acceptable use of Technology Guidelines

The purpose of the acceptable technology use guidelines is to educate students about the potential dangers and benefits of using the internet and technology for learning and communication. The school expects all staff and students to respect each other's digital rights and privacy and to prevent any form of cyber bullying from anyone inside or outside the school.

The acceptable use of technology guidelines for students explains what students are expected to do and not to do when using devices, internet, and digital technology on the school grounds.

The goal is to promote safe, responsible, and ethical online behavior while creating a positive digital learning environment.

These guidelines apply to all students enrolled in the school and cover the use of school-provided devices, personal devices brought onto the premises, and internet access provided by the school.

1. General Guidelines

1.1 **Educational Purpose**: The primary purpose of the use of technology at school is for educational activities, assessment, research, and learning. Students are expected to use online resources responsibly to enhance their academic experience.

1.2 **Responsible Behavior**: Students must exhibit responsible and ethical behavior online, respecting the rights and well-being of others. Any online activity that disrupts the learning environment or infringes upon the rights of others is prohibited.

1.3 **Privacy and Security**: Students are responsible for maintaining the privacy and security of their personal information and login credentials. Sharing passwords or attempting to access unauthorized accounts constitutes a breach of this guideline.

2. Wi-Fi / Internet Access on the devices

2.1 **School Provided Devices**: Students using school devices for accessing Wi-Fi/internet must adhere to the technology usage guidelines. School devices are intended for educational purposes, and their use will be monitored to ensure compliance.

2.2 **Personal Devices**: Students bringing personal devices to access the internet as a part of BYOD policy to the school should use them responsibly for educational purposes. Personal devices must not disrupt the learning environment or fail to adhere to these guidelines.

3. Prohibited Activities

The following activities are strictly prohibited and follow the laws in:

3.1 **Cyberbullying**: Cyberbullying refers to any intentional, aggressive act conducted using electronic means, with the purpose of harming, harassing, or intimidating others within the school community. Engaging in any form of cyberbullying is prohibited.

3.2 **Inappropriate Content**: Accessing, downloading, or distributing inappropriate content, including but not limited to explicit material, hate speech, or violence, is not allowed.

3.3 **Hacking and Unauthorized Access**: Attempting to hack into computer systems, networks, or unauthorized access to data is prohibited. The UAE has stringent cybercrime laws, and unauthorized access to computer systems, hacking, and other cyber offenses are treated seriously.

3.4 **Copyright Violations**: Students must respect copyright laws and refrain from unauthorized downloading, sharing, or distribution of copyrighted materials/software. The UAE has laws protecting intellectual property, and this extends to software. Unauthorized distribution or use of copyrighted software may be subject to legal action.

3.5 **Malicious Software**: Intentionally introducing or spreading malicious software, viruses, or any form of malware is prohibited.

3.6 **Invasion of Privacy**: Prohibits activities like photographing others without permission and managing electronic photos without consent, underscoring the importance of respecting personal privacy.

3.7 **Defamation**: Forbids the dissemination of news, photos, scenes, comments, or statements that, even if true, could harm an individual's or entity's reputation.

3.8 **Amending or Processing for Harmful Purposes**: Restricts the alteration or processing of records, photos, or scenes with the intent of defaming, offending, attacking, or invading the privacy of others.

3.9 **VPN**: The use of Virtual Private Network (VPN) technology is strictly prohibited under the BYOD policy in the school setting. Any attempt to bypass network security measures or access unauthorized content through VPNs is a violation of this policy and may result in disciplinary action.

4. Monitoring and Consequences for Violations

4.1 **Monitoring**: To ensure a secure online environment, the network and internet usage is monitored by a firewall.

4.2 **Device Inspection**: Students may be selected at random to provide their device for inspection. Inappropriate content will be removed, students who refuse to remove inappropriate content will not have use of their device at school until it has been removed.

4.3 **Disciplinary Actions**: Violations of this policy may result in disciplinary actions, including but not limited to loss of internet access, counseling, or, in severe cases, suspension from school.

4.4 **Device Confiscation**: In cases of serious policy violations, school staff may confiscate devices to ensure a safe learning environment.

4.5 **No Permission**: Use of airdrop or any apps which interferes with the school IT functioning infrastructures are not permitted and if found will be dealt strictly.

5. Reporting Incidents

The policy aims to protect victims and address the behavior of perpetrators by establishing clear procedures for reporting incidents, including cyberbullying. This section outlines whom to contact and the necessary information to provide.

5.1 **Reporting Procedure**: Students who witness or experience any violation of these guidelines must report the incident promptly to a teacher or school staff member.

5.2 **Anonymous Reporting**: Anonymous reporting channels will be provided to encourage students to report incidents without fear of retaliation.

5.3 **Investigation Process**: Upon receiving a report, the school initiates an investigation process to address the incident promptly.

6. Education and Awareness

The school will implement educational programs to teach students about internet safety, responsible online behavior, and the potential risks associated with online activities.

6.1 **Workshops and Seminars**: Regular workshops and seminars will be conducted to keep students informed about evolving internet trends and potential threats.

6.2 **Monitoring at Home**: Parents will be informed about the school's technology usage guidelines and encouraged to participate in educational programs to support responsible internet use at home. Parents are encouraged to monitor their child's internet use at home and reinforce responsible online behavior.

6.3 **Cyberbullying awareness**: Raise awareness about the consequences of cyberbullying, the importance of responsible online behavior, and the school's commitment to creating a safe environment.

6.4 **Positive online culture**: Conduct regular awareness campaigns involving students, staff, and parents to promote a positive online culture.

6.5 **Integrate cyberbullying in curriculum**: Integrate cyberbullying awareness and prevention into the school curriculum to ensure continuous education on the topic.

6.6 **Copyright**: Copyright, plagiarism, AI, Deep-Fakes are not permitted. Students need to follow the UAE and Board regulations regarding the same.

10. Student's Roles, Responsibilities and , and Guidelines

Students are responsible for ensuring the appropriate use of personal devices within the school premises. To achieve this, they must:

1. Complete training to understand and adhere to the BYOD Policy.
2. Ensure their BYOD device has the required apps/software installed as specified by the school and maintain software upgrades.
3. Use only licensed software provided by the school for educational purposes.
4. Ensure their device battery is fully charged before coming to school for daily use, has sufficient storage space, and is kept in secure casing. Device charging is not permitted inside the school.
5. Adhere to general school rules regarding behavior and communication in accordance with the school's 'Code of Conduct.'
6. Monitor activity on their accounts (e.g., MS Teams) and report any behavior inconsistent with the school's 'Code of Conduct.
7. Utilize technology and devices in a responsible and ethical manner.
8. iPads/Tablets with cellular connections/eSIM must have this feature turned off and only connect online through the school Wi-Fi network.
9. Keep iPads/Tablets in silent mode while on school premises, unless allowed otherwise by a teacher.
10. Mobile phones are not allowed as learning tools and in school.
11. Games and Web-based activities are not permitted in school campus.
12. The devices should be used only as per the instruction of the teachers. Devices should be kept in the device box when not in use.
13. Promptly report any technical issues to the class teacher.
14. Protect their devices by promptly reporting any security problems to their teacher/IT administrator.

15. Refrain from installing any software that compromises the safety and security of the system, such as VPNs, social media, and games.
16. Headphones and ear-pods are permitted to be used only during the designated activities and assessments as permitted by the teacher.
17. Immediately report any damages to their teacher for investigation and notification to IT administrator and parents.
18. Use the internet safely and appropriately, reporting any inappropriate or offensive websites to their teacher for blocking.
19. Utilize school-sanctioned online web-based platforms to enhance education and facilitate collaborative study habits among students.
20. Always use their own login account and password, avoiding using another individual's account.
21. The network will block all connections deemed inappropriate, including VPN, social media and games. connections. Ensure VPNs are uninstalled while at school.
22. Students are to follow the digital safety guidelines as per the School Policies and UAE Laws and regulations.

Prohibited Activities:

The BYOD policy explicitly prohibits certain activities to ensure a safe and secure digital environment for all students. The following activities are not allowed under any circumstances:

Unauthorized Installations and Content:

- Students must not install any unauthorized software on school devices.
- Students must not create, share, or access content that is illegal, copyrighted, or inappropriate. This includes explicit material, hate speech, or violence.

Security and Privacy Violations:

- Students must not take or share photos or videos of other students without their consent or teacher approval. This applies to any school-related activities or events, whether on or off campus.
- Students must not use any VPN or proxy server to access blocked or restricted websites or services. This is against the law in UAE and can result in imprisonment and fines.
- Students must not use their devices to break any school policies, national or federal laws, or commit any illegal acts.
- Students must not change their device settings or download any apps at school without permission from their parents and teachers.
- Students must not store any personal or confidential information of their parents on their devices.

Communication and Behaviour:

- Students must not access, send, or post any content that is offensive, profane, threatening, pornographic, obscene, religious, or sexually explicit. This includes any form of online communication, such as email, chat, social media, or gaming platforms.
- Students must not use the school internet or email accounts for personal purposes, such as online shopping, academic cheating, or gaming, without school permission.

- Students must also respect the privacy and security of other students' accounts, files, or data and not attempt to access them without authorization.
- Students must not use any anonymous or false communication platforms to deceive, harass, or bully others. Students must also be careful about sharing their personal information online and report any suspicious or inappropriate contacts.
- Students must not participate in any form of cyberbullying or online harassment. This includes sending or posting hurtful, hateful, or harmful messages or images about others.

Legal and Ethical Violations:

- Students must not use the school internet or email accounts for any illegal activities, such as financial fraud, electronic forgery, or identity theft.
- Students must not attempt to hack into computer systems, networks, or gain unauthorized access to data.
- Students must abide by the laws and regulations regarding the use of digital resources and respect the intellectual property rights of others. Students must not download, share, or distribute any copyrighted materials without permission.
- Students must not introduce or spread any malicious software, viruses, or malware that could damage or compromise the school system or network. Students must also not use the school system to access unauthorized or restricted information resources.

Classroom Disturbances:

- Accessing and using non-educational internet/app-based games during class time is prohibited.
- Use of social media and messaging services within school time (e.g., Facebook / X / Snapchat / Instagram / Tiktok / Discourse / any artificial intelligence enabled chats) is prohibited.
- Gaining access to other students' accounts, files, and/or data is prohibited.
- Participation in fraudulent or other illegal behavior is prohibited.
- Playing loud or disruptive audio or video content without permission of the teacher.
- Vandalism of personal, other students', or the school's technology is prohibited.
- Disregarding teacher instructions regarding device usage during specific activities.
- Engaging in unauthorized communication with peers during class time

Any observed activities outlined above will be logged in the INCIDENT module of the school management system and reported to parents, with further action taken.

11. Responsibilities of Parent / Guardian

Students Parents and guardians are integral to the success of the BYOD program and are entrusted with key responsibilities. They play a pivotal role in ensuring the online safety of their children, and various resources offer advice on monitoring computer use at home.

As part of the school's BYOD program, we request that parents and guardians:

1. **Guidance and Awareness**: Provide children with guidance to ensure understanding of the acceptable use of the internet and digital resources.
2. **Establishing Standards**: Set clear standards for device use at home, promoting responsible behavior.
3. **Damage and hazards**: Take responsibility for any mistreatment, breakages, or loss of their child's device.
4. **Insurance Consideration**: Consider obtaining accidental damage and theft insurance to cover potential device damage.
5. **Parental Controls**: Proactively configure parental control options on their child's device.
6. **Device Identification and Maintenance**: Ensure the device is labeled with the child's name, and maintain a record of its serial number, regularly synced/backed up, and properly maintained.
7. **Technical Support**: Address technical concerns, including device malfunctions and warranty claims, extending beyond network-related issues.
8. **Communication and Supervision**: Engage in open communication with children to establish standards for device and internet use at home, emphasizing supervised usage. Monitor students' devices at home as well.
9. **Shared Responsibility**: Acknowledge that both parent and child share responsibility for the device, with the school not assuming liability for mistreatment, breakages, vandalism, or loss.
10. **Age-Restricted Sites**: Understand that students under 13 should not participate in age-restricted Social Networking sites and Games without parental consent.
11. **Communication Channels**: Refrain from contacting children on their devices during school hours and use school reception or appropriate email channels for communication.
12. Parents will ensure that students do not carry their mobile phones to school.

Recommended Resources for Parents/Guardians:

- **Thinkuknow** (https://www.thinkuknow.co.uk/parents): Provides guidance for parents on online safety.
- **Safer Internet** (https://www.saferinternet.org.uk/): Offers tools and advice to promote a safer online environment for children.
- **Childnet** (https://www.childnet.com/): Resources for parents to help children stay safe online.
- **Anti-Bullying Alliance** (https://www.anti-bullyingalliance.org.uk/): Addresses issues related to online bullying and provides support.
- **SPCC** (https://www.nspcc.org.uk/): Offers resources on online safety and protecting children from harm.
- **Cyber Angels** (https://www.nspcc.org.uk/): Provides information and support on internet safety.

12. Responsibilities of School

The school plays a foundational role in the BYOD Program, ensuring not only educational value but also social responsibility and safety for its students. As part of the program, the school will:

1. **Technical Infrastructure and Support:**
    - Provide a safe and secure network structure for BYOD devices.
    - Ensure reliable internet access for educational purposes.
    - Offer an Office 365 email account and access to Office365 apps with a student license.
2. **Security and Safety:**
    - Educate students on routines and expectations for the safety and care of their devices.

- Train teachers on the use of devices and ensure all staff are familiar with BYOD program processes.
- Train teachers on cyber safety and allocate curriculum time for teaching students about being cybersafe.
- Provide filtered internet access, monitor student use, and enforce the school's Internet Usage Policy.
- Implement firewalls to create a safe cyber environment.
- Block offensive, profane, threatening, pornographic, obscene, or sexually explicit materials.

3. **Educational Support:**
    - Setup a DGCC (Digital Governance and Compliance Committee) to educate students, staff, and parents on safety guidelines for device use.
    - Ensure that staff carefully select online content for students, and at times, allow students to create accounts for educational resource sites.
    - Enforce guidelines for posture, rest periods, stretching, noise, and other environmental hazards during device use.
4. **Policy Enforcement and Communication:**
    - Enforce the BYOD policy by having teachers monitor students' use of personal devices in the classroom.
    - Require parents and students to sign and adhere to the BYOD policy before bringing personal devices to school.
    - Provide regular reminders and training on the responsible use of personal devices to students and staff.

13. Compliance with Laws

Students who join the BYOD program must follow the laws and regulations set by the United Arab Emirates. The UAE has enacted several laws and policies to enhance its cybersecurity and protect its citizens and residents from online threats and crimes. The Federal Decree Law No. 34 of 2021 on Combating Rumours and Cybercrimes provides a comprehensive legal framework to address the misuse and abuse of online technologies, such as hacking, spreading false information, and violating privacy. The law also lists the offences and penalties for cybercrimes and aims to safeguard the UAE's national security and interests. Additionally, the UAE's National Cybersecurity Strategy and the Dubai Cyber Security Strategy outline the goals and initiatives to create a safe and strong cyber infrastructure in the country. These laws and policies reflect the UAE's commitment to ensuring digital trust and security for its people and businesses.

The Cybercrime Law (Federal Law No. 5 of 2012 forbids unauthorized access, disclosure, or destruction of data and software, as well as cyber fraud, identity theft, and cyber terrorism. The Data Protection Law (DIFC Law No. 5 of 2020 regulates the collection, processing, transfer, and security of personal data. Moreover, the Electronic Transactions and Commerce Law (Federal Law No. 1 of 2006 confirms the validity of electronic transactions, contracts, signatures, and records. Students must also abide by the Telecommunications Regulatory Authority's policies, which set standards and rules for the use of telecommunications services and devices in the UAE.

Students who use their own devices for educational purposes must comply with all applicable laws and regulations, including those related to computer software, applications, databases, and similar works. Students must not use their devices to access, store, transmit, or distribute any illegal, infringing, or unauthorized software or applications. Students must respect the intellectual property rights of others and obtain any

necessary licenses or permissions before using or sharing any software, applications, or databases. Students who violate any laws or regulations through their use of personal devices may be subject to disciplinary action, legal liability, and termination of BYOD program. This includes, but is not limited to, the violation of Federal Law No. 38 of 2021 on Copyrights in the UAE.

Non-compliance with these laws and regulations can lead to serious consequences, such as legal prosecution, suspension, or expulsion. It is vital for students to realize that respecting academic integrity and ethical conduct applies to their use of technology. By adhering to the school's BYOD policy guidelines, students not only meet a legal requirement but also help to ensure the safety, security, and integrity of the school community. Awareness of these laws and responsible technology use not only safeguards individuals but also fosters a culture of respect for intellectual property and digital rights within the academic setting.

14. BYOD Technical Support

As part of the BYOD Program, the school is committed to providing limited technical support to assist students with the following:

1. Connecting to the school's Wi-Fi/internet.
2. Installing recommended applications.
3. User profile management.

Please notify the IT support team at **itsupport_secondary@apple.sch.ae** for secondary campus and **itsupport_primary@apple.sch.ae** for the Primary campus.

1. You believe your password has been compromised or if you have been asked to provide your password to another individual.

2. You suspect you have received a phishing email. Each reported instance will be thoroughly investigated by the IT department.

Feedback from students and parents is actively sought to inform the review process. Please reach out to us for any concerns or suggestions.

15. Promotion of the Policy

To foster a culture of responsible and secure technology use, the school is committed to promoting the Bring Your Own Device (BYOD) policy through various initiatives. Orientation sessions at the commencement of each academic year will educate students, staff, and parents about the policy's key aspects, while regular distribution of informational circulars will reinforce its guidelines. Workshops and information sessions for parents, coupled with teacher training, will ensure a comprehensive understanding and support system. In addition, the policy will be promoted through coffee mornings for parents, and workshops for both parents and students across the entire school. Engaging events like technology fairs and competitions centred around responsible device use will further emphasize the benefits of the BYOD policy, encouraging a collective commitment to a secure and productive digital learning environment.

16. Policy Review

The BYOD policy undergoes an annual review to ensure its relevance, effectiveness, and alignment with emerging educational technologies and security measures.

17. Conclusion

The BYOD policy at Apple International School is a comprehensive framework aimed at fostering responsible, secure, and educational use of personal devices within the school environment. It reflects our commitment to providing students with a cutting-edge learning experience while maintaining a safe and secure digital environment.

This policy is subject to periodic reviews and updates to align with the evolving landscape of educational technology and security standards. All stakeholders are encouraged to participate in the feedback process to ensure the BYOD program's continued success at Apple International School.

ACKNOWLEDGMENT

* Any mobile phones including Smartphones and smartwatches are not permitted (However if the students are self-walkers they needs to get the permission from respective section head and proceed accordingly). In case if the phone is found misused it will be confiscated and will be given only at the end of the Term to parents.) Devices must not have ESIM/SIM cards installed.

*Students must install Office 365 applications (Word, Excel, PowerPoint, Teams) on their devices using the school-provided Office 365 account.

*The school is not responsible for the security, maintenance, or repair of personal devices. Students are expected to take reasonable precautions to safeguard their devices.

* Cyberbullying refers to any intentional, aggressive act conducted using electronic means, to harm, harass, or intimidate others within the school community. Engaging in any form of cyberbullying is prohibited.

* Students must not access, send, or post any content that is offensive, profane, threatening, pornographic, obscene, religious, or sexually explicit. This includes any form of online communication, such as email, chat, social media, or gaming platforms.

* Attempting to hack into computer systems, networks, or unauthorized access to data is prohibited. The UAE has stringent cybercrime laws, and unauthorized access to computer systems, hacking, and other cyber offenses are treated seriously.

* Students may be selected at random to provide their device for inspection. Inappropriate content will be removed, and students who refuse to remove inappropriate content will not have use of their device at school until it has been removed.

We kindly request you to read and Knowledge the complete BYOD policy for more information.

Disclaimer: The school is not responsible for any loss, damage, or theft of personal devices.

By signing this policy, the student and parent/guardian understand and agree to abide by the guidelines outlined in this policy.

Disclaimer: The school is not responsible for any loss, damage, or theft of personal devices.

By signing this policy, the student and parent/guardian understand and agree to abide by the guidelines outlined in this policy.

Signed: _____(Student with AIS ID) Date: _____