BYOD Guidelines

At Tokyo West International School (TWIS), technology, such as MacBooks and iPads, are fully employed in the classrooms. The program, "Bring Your Own Device" (BYOD), began in April 2022. Access to technology will increase class engagement and develop the skills required to thrive in the 21st-century.

Video game devices with internet access (Nintendo Switch, PSP, etc…) are not permitted at any time. iPhones and other smartphones are not permitted for classroom use.

Recommend Devices

【Primary School 】

Grades 3 through 6 students are invited to bring one of the below models of iPads with the most recent operating system version and all security updates installed.

Any of the following models, version 2018 or later:

• iPad

• iPad Air

• iPad Pro

Recommended 128GB or more of storage and Wi-Fi access. Mandatory protective case and labeling of students ' names on both the case and the iPad.

To help you decide on the most suitable model, kindly visit:

https://www.apple.com/jp/ipad/compare/

https://www.apple.com/jp/ipad/

【Middle School 】

Grades 7 through 9 students are invited to bring one of the below models for MacBook. In case Grades 3 through 6 students choose to bring the MacBook, they are also invited to bring one of the following models.

version 2018 or later:

• MacBook

• MacBook Air

• MacBook Pro

Recommended 8GB or more of memory, 128GB or more of storage. Mandatory protective case and labeling of students ' names on both the case and the laptop.

To help you decide on the most suitable model, kindly visit:

https://www.apple.com/jp/mac/compare/

https://www.apple.com/jp/mac/

Repair, Maintenance, and Security

The repair, maintenance, and security of the devices are the responsibility of the students. We recommend that families inquire about their property insurance coverage and make allowances as needed to comprehensively cover their child's device. Additionally, students must ensure that their devices are fully charged for each school day.

Software

Students should keep their devices up to date with the latest operating systems. Students must be able to install software independently. Most work is done in Google Workspace for Education (Google Docs, Sheets, Slides) on laptops. Students can also use the iWork software (Pages, Numbers, Keynote), which comes free with a purchase of a MacBook or iPad.

BYOD Policy

Use of personal devices:
- The use of personal devices on school grounds is at the discretion of the teachers and staff. All students MUST use their devices as directed by their teachers and staff.
- The use of personal devices is not to be a distraction in the classroom or private study areas used by teachers or pupils.
- Students are not allowed to use personal devices outside of the classroom unless they are being used during school visits, field trips, or outside activities.
- Playing games on devices is NOT permitted unless the game is used for educational purposes and/or authorized by the teacher.
- Approved devices must be in silent mode while on the school campus, unless otherwise allowed by a teacher. Headphones may be used with the teacher's permission.
- Devices should not be used to cheat on assignments, quizzes, or tests, or for non-instructional purposes (such as making personal phone calls and text messaging).
- All students are required to check their personal devices daily to ensure that the device is fully charged and free of any malicious content such as viruses and malware that may compromise the security of the school's network. These checks must be completed before bringing the device to school.
- To conform to health and safety guidelines, no defective or damaged devices should be brought into the school.
- No gaming hardware (such as gaming mouse, keyboards, headset, etc.) will be allowed at school, unless explicitly authorized by the teacher. Any gaming material brought to school will be confiscated and returned at the end of the term.
- It is not allowed to share devices with other students unless teachers give permission to do so.

Essential Agreement

1. Gadgets should not be used for gaming or inappropriate content.
2. Should there be a student outside of the classroom using a gadget, the teacher should investigate what the student is doing and why they are outside of their classroom. The teacher should then ask the student to go back to their classroom and should report to the HR teacher what the student was doing on the gadget.
3. No gadgets outside of the classroom during morning and afternoon recess If the gadgets are to be used, the students must stay in their classrooms.

Lost, Stolen, or Damaged Devices:

1. Each user is responsible for his/her own device and should use it responsibly and appropriately. Tokyo West International School takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices.
2. Tokyo West International School is not responsible for any possible device charges to your account that might be incurred during approved school-related use.
3. Tokyo West International School is not responsible for maintaining or troubleshooting students' personal devices.

Network safety and harmful behaviors:

1. All users agree not to exploit technological resources, interfere with another student's use of the resources, or use technology resources with the intent of causing harm to others.
2. Students may not use devices to record, transmit, or post photographic images or videos of a person or persons on campus during school hours or school activities, unless otherwise allowed by a teacher.
3. Bringing a device that infects the network with a virus, Trojan, or a program designed to damage, alter, destroy, or provide access to unauthorized data or information is strictly forbidden on the premises.
4. Processing or accessing information on school property related to "hacking." This includes downloading programs to bypass or alter security, accessing, and setting up proxies.

Note:

Tokyo West International School (TWIS) is authorized to collect and examine any device that is suspected of causing technological problems or is the source of an attack or virus infection. Students and parents should be aware that devices are subject to searches by school administrators if the device is suspected of a violation of the student code of conduct. If the device is locked or password-protected, the student will be required to unlock the device at the request of a school administrator.