DEVICE POLICY

JV VISION STATEMENT

To create the leaders of tomorrow who are physically, psychologically, intellectually, and ethically strong, to overcome all challenges with ease in every sphere of life.

IB MISSION STATEMENT

The International Baccalaureate aims to develop inquiring, knowledgeable and caring young people who help to create a better and more peaceful world through intercultural understanding and respect. To this end the organization works with schools, governments and international organizations to develop challenging programmes of international education and rigorous assessment. These programmes encourage students across the world to become active, compassionate and lifelong learners who understand that other people, with their differences, can also be right.

BRING YOUR OWN DEVICES (BYOD) POLICY

Technology is an essential part of modern life, and its role in education is no different. At Jain Vidyalaya, we are dedicated to creating a learning environment that leverages technology to enhance learning, unlock student potential, and foster global connections. Our campus is equipped with high-speed internet access in all areas, ensuring that students and staff can seamlessly integrate technology into their educational experience. Students are also encouraged to bring their own devices (BYOD) to support personalized learning and access to digital resources.

As digital natives, our students grow up immersed in technology, and the BYOD policy is designed to ensure they develop the digital literacy skills necessary to excel in today's world. This initiative empowers all members of our school community to thrive in the ever-evolving digital landscape.

learning support BYOD

Student-centered learning is a core value of every IB World School, and the BYOD policy supports this philosophy by empowering students to take greater ownership of their learning journey and develop the attributes outlined in the IB Learner Profile.

At Jain Vidyalaya, our goal is for students to engage with technology as a tool for learning, rather than simply learning from technology. The BYOD program encourages the development of essential contemporary skills, including:

- Accessing, filtering, and processing information
- Planning and organizing
- Making informed choices and decisions
- Facing challenges and problem-solving

- Taking risks and overcoming obstacles
- Collaborating and sharing
- Communicating effectively
- Being creative and innovative
- Reflecting on learning experiences

This policy applies to any non-school-owned or supplied device used to access the school's wireless network. Its purpose is to set clear guidelines and procedures to ensure the safe use of personal devices in school and to maintain the integrity of the school's network.

Devices - suitable for BYOD.

At Jain Vidyalaya, our BYOD model follows the "Bring Your Own Standard Device" approach, where students are required to procure a device from a limited selection that meets standardized requirements set by the school. While the device is fully funded and owned by the student, it is managed by the school to ensure compatibility with the learning environment. This model allows both parents and students to choose a device that fits their budget and preferences, while still fulfilling the academic and technical needs of the school.

IBCP (Grade: 11 & 12) - Laptop/MacBook

Smartphones are not considered suitable devices due to screen size, storage limitations, and function restrictions.

Below specifications for the device are advised to be used.

Windows Laptop:

1. Device (laptop) not older than 5 years.
2. Device (laptop) with 4GB of RAM.
3. Device (laptop) with a 4 + hour battery life.
4. Device (laptop) supporting WIFI.
5. Device (laptop) with Windows 7 or above.
6. Device (laptop) with up to date anti-virus software

Apple Laptop:

1. Device (laptop) not older than 5 years.
2. Device (laptop) running with the latest OSX.
3. Device (laptop) with at least 4GB of RAM (8GB recommended for MacBook Pro).
4. Device (laptop) that has a 4 + hour battery life.
5. Device (laptop) supporting WIFI.

Software:

- Office package must be installed on the device.
- Additional softwares/applications list that is required for learning will be intimated/provided by the facilitators.

Restrictions to use the device:

The use of personal devices at Jain Vidyalaya is strictly for instructional purposes and is subject to the teacher's discretion. Additionally, wireless access is limited to internet use only.

Students will not have access to other school systems or printers.

Using the school's wireless network requires personal responsibility and adherence to all school rules and policies.

Technical support:

All students will receive the necessary Technical support and guidance to set up passwords and access the internet and also in any technical difficulties.

If the device cannot be repaired, a replacement device will be provided by the school, solely for use within the school premises, and subject to adherence to all school protocols and policies.

Acceptable Use Policy

All students and parents or legal guardians must review and agree to the Acceptable Use Policy.

1. General Guidelines

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.

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.

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

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:

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.

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

Hacking and Unauthorized Access: Attempting to hack into computer systems, networks, or unauthorized access to data is prohibited.

Copyright Violations: Students must respect copyright laws and refrain from unauthorized downloading, sharing, or distribution of copyrighted materials/software.

Students must provide a proper citation and references while using online material or content.

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

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

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

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.

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

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

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.

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.

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

No Permission: Use of airdrop or any apps which interfere 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 behaviour of perpetrators by establishing clear procedures for reporting incidents, including cyberbullying.

This section outlines whom to contact and the necessary information to provide.

Reporting Procedure: Students who witness or experience any violation of these guidelines must report the incident promptly to the faculties or school staff members.

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

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 and prompt usage of the devices.

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

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.

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

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

Copyright: Copyright, plagiarism, AI are not permitted.

Guidelines for Students

1. The student is fully responsible, at all times, for their personal laptop. School is not liable for any loss/damage/theft or any monetary charges that may occur while the student is using the device.
2. Approved devices must be in silent mode while on school campus unless otherwise allowed by a teacher.
3. Students are required to bring their own headphones. Headphones may be used with teacher **permission**.
4. Devices may not be used for non-instructional purposes (such as making personal phone calls and text messaging).
5. Devices should be sufficiently charged before the start of school every day.

6. 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.
7. Devices may only be used to access computer files on internet sites which are relevant to the classroom curriculum.
8. Students must ensure they have the latest software installed on their devices, relevant to the subject area.
9. It is the student's responsibility to maintain sufficient memory capacity on their device to enable its use for educational purposes.
10. Devices must have appropriate protection/cases allowing easy carrying of the devices.
11. Devices must have a secure **login and password**.
12. If reasonable belief exists that the student has violated the conditions of this agreement the student's device may be inspected and/or confiscated. Subsequent or additional disciplinary action involving misuse of technology may extend to loss of technology privileges or further action as determined by the Head of School.
13. Students are expected to bring in their device each day on the assumption that the teacher may elect to use them for their lessons.
14. For safety reasons, students are not allowed to use their electronic devices outside the classroom except with the permission of a teacher or at designated work tables.
15. Electronic devices are not permitted in the Canteen Area.
16. Students are not permitted to use electronic devices outside during lunch.
17. While in the library, students may use their laptops for educational purposes.
18. The use of a mobile phone or ear buds at school are not permitted.
19. Use of Calculator outside the classroom is not permitted.

Students and Parents/Guardians acknowledge that:

- The school's network filters will be applied to a devices' connection to the internet and any attempt to bypass the network filters is prohibited.
- The School is 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.

- All students involved in the BYOD program will supply their own devices and be responsible for its safety, whilst on the school premises.
- Students, Staff and Parents/Guardians are prohibited from knowingly bringing a device on premises that infects the network with a 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 systems.
- The School is 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.
- School is not responsible for loss or damage of student's personal devices or cases.
- Any student in breach of this BYOD policy will result in confiscation of the device.

Lost, Stolen, or Damaged Devices:

- Each user is responsible for their 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.

Responsibilities of the school:

- Provide a safe network structure and access to the Internet that enables the comprehensive use of the laptop.
- The school will make every effort to ensure that students understand the routines and expectations for the safety and care of the devices brought to school.

Teachers will help children to identify how to keep personal devices secure, but children have the final responsibility for securing their devices.

- Provide support to access the school's systems and applications (if necessary).
- Provide a temporary laptop for students to borrow if their laptop is not working (Using Computer Lab Systems)
- Provide technical support and advice to fix hardware and software issues which can be resolved without dismantling the laptop's parts.
- The school shall not be liable for any damages occurring on the school's premises.

Acceptable use of Technology Guidelines

The purpose of the acceptable technology use guidelines is to educate students on the potential risks 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 while actively preventing any form of cyberbullying, whether from individuals inside or outside the school.

These guidelines outline what students are expected to do and avoid when using devices, the internet, and digital technologies on school grounds.

The aim is to foster safe, responsible, and ethical online behavior while promoting a positive digital learning environment.

These guidelines apply to all students enrolled at the school and cover the use of both school-provided devices, personal devices brought to campus, and any internet access provided by the school.

Disciplinary Steps for Misuse of Electronic Devices

Level 1: Non-habitual and/or compliant with consequences: The staff will confiscate the device and submit it to the Head of School (HOS)/CPC, where it will remain for the rest of the day

Level 2: Habitual and/or non-compliant: Staff will confiscate the device and pass it to the HOS for the remainder of the day.

A detention will be issued by the Head of School (HOS)/CPC and the action will be recorded in the school's online learning management system.

Level 3: Referred to Administration: Staff will confiscate the device and pass it to the Head of School (HOS)/CPC for consultation with administration.

The office will be in touch with the parent/guardian to address the issue and the device will be held in the office for the parent/guardian to pick up.

Further violation may result in a suspension from school.

Failure to surrender devices when asked to do so by a member of staff will result in a referral to the administration office.

Students who have had their computers confiscated for the day are not excused from completing their work.

The student is responsible for using their electronics appropriately during school time.

Students are encouraged to ask a teacher if they are unsure whether they are using their electronic device appropriately.

Use of calculators in IB DP:

A calculator will not be permitted for IB DP examinations if:

- it does not meet the minimum requirements for calculators for that subject.
- it includes functionality that is unique to the prohibited calculators listed in this document, most predominantly CAS functions.
- it includes additional elements, for example third-party applications or student generated notes, which are not removed (via a reset) or blocked (via an examination mode).

Permitted calculators

Casio	FX-9860GII / FX-9860GII SD / FX-9860G AU PLUS updated to the latest operating system for IB examinations in "Examination Mode (for IB)"
	FX-9750GIII / FX-9860GIII / Graph 35+ EII updated to the latest operating system for IB examinations in "Examination Mode (for IB)"
	FX-CG50 / FX-CG50AU / FX-CG20 / Graph 90+E updated to the latest operating system for IB examinations in "Examination Mode (for IB)"

Ensure, via the Casio website, that your device has the latest operating system. https://edu.casio.com/download_service/download/ib/

All recommended Casio calculators must be initialized and reset.

Prohibited calculators

The following models are not allowed in examinations under any circumstances.

<table>
<tr><td rowspan="3">Texas Instruments</td><td>TI Voyage 200 (all versions)</td><td>TI 89 (all versions)</td></tr>
<tr><td colspan="2">Older CAS models:
• TI-Nspire CX CAS
• TI-Nspire CAS</td></tr>
<tr><td colspan="2">TI-Nspire models that are not updated to the latest operating system</td></tr>
<tr><td>Hewlett Packard</td><td colspan="2">HP 38-95 (all versions)</td></tr>
<tr><td rowspan="3">Casio</td><td>Classpad (all versions) / FX CG500</td><td>Graph 100</td></tr>
<tr><td>FX 2.0 (all versions)</td><td>FX 9970 (all versions)</td></tr>
<tr><td colspan="2">Devices with an “Examination Mode” that are not updated to the latest operating system</td></tr>
</table>

Notes:

- Any devices (Calculators) with unrestricted/student accessible WiFi functionality are not permitted.
- Other calculators which have advantageous features that do not appear on any of the permitted models and/or have functionality that is exclusive to the prohibited calculators (and not blocked during the examination) are not allowed.
- Students may not use or store data/notes, programs or flash (ROM) applications (Apps) in their calculators that may assist them in an examination by removing the need to recall facts or formulae.

Policy Review:

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

Team involved while the creation of the Policy:

- ✔ HOS
- ✔ CPC
- ✔ Core, DP, CRS teachers
- ✔ Librarian

Bibliography

Whole School BYOD Policy.docx (eischools.ae)

265212-bskl-byod-policy-for-secondary-students-.pdf (nordangliaeducation.com)

BYOD-Policy-23-24.pdf (apple.sch.ae)

https://resources.ibo.org/data/d_4_gen4d_sup_2403_1_e.pdf

https://edu.casio.com/download_service/download/ib/

THE BOYD PARTNERSHIP AGREEMENT

We have reviewed and understand how the BYOD policy will enhance student-centered learning at Jain Vidyalaya. We commit to collaborating with the school as per the agreement outlined below. We also recommend that parents ensure devices are fully insured, serial numbers are recorded, and, where possible, tracking or location software is installed to safeguard the devices.

Agreement	**Please Tick**
We agree that students are responsible for the safety, security loss or damage of their device. The school cannot be held responsible for student devices.	
Devices should only be used for learning purposes, as instructed by a teacher. Using the device in a way that disrupts the learning of others will not be tolerated.	
Users must power off and put away personal devices if directed to do so by teachers or school administration.	
Users must abide by all school policies when using their own devices.	
Users are responsible for the use of their personal device on the School network at all times.	
The school is unable to support any technical issues and/or upgrades of the device.	
Users should practice caution when allowing others to access their personal device. All liabilities remain with the user.	
It is expected that students arrive at school with their devices fully charged.	
It is expected that apps are downloaded at home and that iTunes accounts are not accessed in school, to protect parents and students financially.	
The use of private wireless connections is not permitted. In school students should only connect to the internet via the school WIFI.	
The use of a device to threaten the sense of security or well-being of others will not be tolerated on or off campus.	

Failure to adhere to the partnership agreement may result in the student being removed from the BYOD programme.

Name and Signature of Student

Name and Signature of Parent