

Jumeira Baccalaureate School

Students' BYOD Policy, Device Access, and Acceptable Use Guidelines

2026 –2027

Policy Title: Students' BYOD Policy, Device Access, and Acceptable Use Guidelines					
Policy Reference code	Revision	Review Date	Reviewed by	Signature	Date of next review
WS20	3	01/05/2026	Richard Drew School Principal		21/5/26
			Shona Gastaldi Head of Primary School		21.05.26
			Lisa Postlethwaite Head of Secondary		21/5/26

Table of Contents

Our Vision, Mission and Core Values.....	3
Vision:	3
Mission:	3
Core values: The 4 R's	3
Rationale	4
Scope	5
Eligibility	6
Approved Devices & Minimum Specifications	7
Purchasing through JTRS	9
Device Access & Connectivity	9
Student Responsibilities.....	10
Parent/Guardian Responsibilities	11
School Responsibilities	12
Acceptable Use Guidelines	13
Acceptable Use (Devices)	13
Acceptable Use (Digital Wellbeing)	14
Monitoring and Consequences	16
Prohibited Activities	16
Device Inspection & Confiscation	17
Consequences	18
Security, Safety, and Liability	18
Reporting	19
Misuse and Disciplinary Action	20
Behaviour Levels and Consequences	20
Agreement and Acknowledgement	21

Our Vision, Mission, and Core Values

Vision:

Our vision is to be a school of good character, excellence and outstanding performance.

Mission:

Our mission is:

- To ignite passion, purpose, and curiosity in our students.
- To promote wellbeing within our community.
- To provide an IB education with high expectations that is innovative, internationally minded, and inclusive.

Core values: The 4 R's

- Responsibility
- Respect
- Resourcefulness
- Resilience

Definitions of our mission and core values:

Our mission:

- **Wellbeing:** promoting self-awareness, self-control, empathy, social skills and personal responsibility.
- **Innovation:** promoting critical thinking; communication; collaboration; and creative problem-solving skills.
- **High expectations:** promoting learner resilience; the capacity to reflect and act on feedback; pride in work; and a belief to exceed.
- **Inclusion:** promoting a diverse learning community; knowing and motivating each learner through differentiation. International mindedness: promoting a respectful attitude to self and others.

Core Values:

- **Responsibility:** I am accountable for my actions and stand up for what is right
- **Respect:** I treat myself, others, and the environment well.
- **Resourcefulness:** I find innovative solutions for positive outcomes
- **Resilience:** I do not give up in challenging situations and help others to do well.

Introduction

Jumeira Baccalaureate School (JBS) is committed to providing an innovative, inclusive, and future-ready learning environment where technology enhances teaching, deepens learning, and supports the development of our students as responsible, respectful, resourceful, and resilient global citizens.

The Bring Your Own Device (BYOD) programme enables students to use their own approved devices to access digital tools, collaborate with peers, and engage with rich, interactive learning experiences both inside and outside the classroom.

This policy sets out the expectations for device use at JBS, ensuring that all students benefit from technology in a safe, secure, and respectful way. It explains the responsibilities of students, parents/guardians, and the school, and outlines the standards of acceptable use that reflect our school's ethos and safeguarding obligations.

The guidelines in this policy apply to all students participating in the BYOD programme, across all year groups where BYOD is implemented, and covers all use of personal devices while on school premises or engaged in school-related activities. Compliance with this policy is a condition for connecting any personal device to the JBS network.

Rationale

At Jumeira Baccalaureate School, we believe that technology, when integrated purposefully, enhances learning, fosters creativity, and prepares our students to thrive in a digitally connected world. The BYOD programme allows students to use familiar, personally owned devices to access school resources, collaborate on projects, and develop digital literacy skills that are essential for lifelong learning.

Our decision to adopt and maintain a structured BYOD policy is grounded in the following principles:

- **Alignment with Vision, Mission, and Core Values**
Our BYOD policy supports our mission to ignite passion, purpose, and curiosity by providing flexible access to technology that promotes Responsibility, Respect, Resourcefulness, and Resilience.
- **Consistency Between Home and School Learning**

- **Digital Citizenship and Safeguarding**

BYOD provides an opportunity to embed responsible and ethical use of technology into daily practice, ensuring that students develop the skills to navigate the online world safely, respectfully, and in compliance with UAE regulations and international best practice.

- **Operational Efficiency and Equity**

Clear expectations for device specifications, software, and connectivity enable consistent teaching delivery and IT support, while ensuring that every student can participate effectively in digital learning. School-owned loan devices (when available) remain available for short-term needs, maintaining inclusivity for all.

- **Future-Readiness**

As technology and curriculum demands evolve, the BYOD framework ensures JBS students are equipped with the tools and habits to adapt, innovate, and succeed in higher education and the workplace.

Scope

This policy applies to all students participating in the Jumeira Baccalaureate School BYOD programme, across all grade levels where BYOD has been implemented. It covers the use of personal devices on school premises, during school-related activities, and when connected to the Student BYOD Wi-Fi network.

The scope of this policy includes:

Device Types - Laptops, tablets, and other approved personal computing devices as specified in the JBS Device Specifications for each grade level.

Approved Use - Accessing school systems, platforms, and learning resources for educational purposes in accordance with the Acceptable Use Guide and JBS Behaviour Management Policy.

Locations and Activities - All classrooms, school facilities, co-curricular activities, excursions, and off-site events where school network access is available or where personal devices are used for learning.

Users - Students, parents/guardians (as custodians of devices for students), and school staff involved in managing, supporting, or monitoring BYOD use.

Timeframe - All times when the device is on school property, connected to the school network, or being used in the context of a school activity, whether during or outside of normal school hours.

This policy works in conjunction with:

- JBS Academic Integrity Policy
- JBS Whole School Behaviour Management Policy
- JBS Safeguarding and Child Protection Policy
- UAE laws and regulations regarding technology use, cybercrime, and online safety

Compliance with this policy is a condition for connecting a personal device to the JBS network and participating in BYOD. Failure to adhere to these requirements may result in the restriction or removal of BYOD privileges, alongside further disciplinary measures as outlined in the JBS Behaviour Management Policy.

Eligibility

Participation in the Jumeira Baccalaureate School BYOD programme is open to all students in year groups where BYOD has been implemented, provided they meet the following requirements:

Year Group Requirements

Grades 3:

- iPads are recommended for Grade 3.
- Accepted devices include iPad with a protective case, screen protector, and headphones. Keyboard (encouraged for typing practice)
- Devices purchased through JTRS for JBS will be pre-configured with safeguarding features, filtered browsing, and school access settings.

Grades 4 and 5:

- All students must bring a device with a keyboard.
- Accepted devices include iPad with detachable keyboard, Windows laptop, or MacBook.
- Please note iPads are not recommended beyond Grade 5 due to compatibility limitations with secondary school software.

Grade 6 and Above:

- Students must bring a laptop (Windows or MacBook).
- iPads are not recommended at this level.
- Minimum specification requirements must be met for processor, RAM, storage, battery life, Wi-Fi compatibility, and security software.
- Please see minimum recommended specifications in the table below.

Approved Devices & Minimum Specifications

To ensure compatibility with JBS learning platforms, school systems, and safeguarding requirements, all student devices must meet the following specifications for their grade level.

We strongly recommend that families purchase device insurance (such as AppleCare for iPads or equivalent coverage for laptops) to protect against accidental damage, theft, or hardware failure. Repair and replacement costs can be significant, and the school is not responsible for these expenses.

Grades 3: Flexible Device Options

Category	Requirement
Accepted Devices	iPad (recommended)
Strongly Recommended	AppleCare (for iPads) or equivalent insurance, Stylus (digital pen)
Recommended Accessories	Protective case, Screen protector, Headphones
Optional	Keyboard (encouraged for typing practice)

Grades 4–5: Device with Keyboard Required

Category	Requirement
Accepted Devices	iPad with detachable keyboard OR Laptop (Windows or MacBook)
Required Accessories	Protective case, Screen protector, Headphones, Stylus (digital pen), Keyboard (mandatory)

Strongly Recommended	AppleCare (for iPads) or equivalent insurance
<i>iPads not recommended beyond Grade 5 due to secondary school software compatibility</i>	

Grades 6 and Above: Laptop Required

Category	Requirement
Accepted Devices	Microsoft Laptop (Windows 10/11) OR MacBook (macOS 14+)
iPads	Not recommended beyond Grade 5
Strongly Recommended	Extended manufacturer warranty or insurance coverage for accidental damage, theft, or loss

Minimum Hardware Requirements

Hardware	Laptop-Microsoft	MacBook-Apple	iPad
OS	Windows 10/11	MacOS 14+	iOS 15.6 or later
Processor	Intel i5 / AMD Ryzen 5	Apple M2 (or equivalent)	Apple M2
RAM	8GB+ RAM	8GB+ RAM	8GB+ RAM
Storage	256GB (SSD/NVME preferred)	256GB (SSD/NVME preferred)	128GB+ Storage
Battery Life	6+ hours	6+ hours	8+ hours
Wi-Fi	Dual band (2.4GHz & 5GHz), WPA2/WPA3 support	Dual band (2.4GHz & 5GHz), WPA2/WPA3 support	Wi-Fi 6 (802.11ax) preferred
Screen	14 Inch or above	13 Inch or above	10 Inch and above
Security	Antivirus	Antivirus	Antivirus

General Requirements for All Devices:

- Devices must be in good working order, with no cracked screens or damaged hardware.
- Devices must support school-approved software and configurations, including safeguarding filters, security profiles, and required educational apps.

General Requirements for All Devices:

- Devices must be in good working order, with no cracked screens or damaged hardware.
- Devices must support school-approved software and configurations, including safeguarding filters, security profiles, and required educational apps.
- Devices must be clearly labelled with the student's full name.
- Students must bring their devices fully charged each day.
- Parents/guardians are responsible for the cost of repair or replacement if a device is damaged, lost, or stolen.

Purchasing through JTRS

We strongly recommend purchasing through JTRS, who offer devices at a discounted rate for JBS families and pre-configure them for school use:

👉 <https://jbschool.jtrs.ae>

Devices from JTRS include automatic safeguarding features:

- They are profiled to only allow access to educational content during school hours.
- Browsing is filtered and monitored while on school Wi-Fi.

Device Access & Connectivity

To maintain a safe, secure, and effective digital learning environment, all student devices connected to the JBS network must adhere to the following access and connectivity requirements:

Network Access:

- Students must connect their devices only to the designated Student BYOD Wi-Fi network.
- *Personal hotspot or mobile data usage is not permitted on school premises.*
- All internet access is filtered and monitored in accordance with JBS safeguarding protocols and UAE regulations.

Authentication and Security:

- Devices must be configured with school-approved security profiles and settings before they are allowed to connect to the network.
- Students must ensure their device operating system and security software are kept up to date to maintain compliance with school security standards.

Prohibited Connectivity Practices:

Proudly
taaleem



- Use of Virtual Private Networks (VPNs) or proxy services is strictly prohibited on campus, as these can bypass the school's safeguarding and content-filtering systems.
- Students must not attempt to circumvent network security measures or gain unauthorized access to restricted resources.

Data Privacy and Safety:

- All activity on the Student BYOD Wi-Fi is subject to monitoring by the IT Department in line with the school's Acceptable Use Guidelines.
- Students must not share their network login credentials with others.
- Any suspected breach of security, suspicious network activity, or exposure to inappropriate content must be reported to the IT Department immediately.

IT Support

- The IT Department provides support for connecting devices to the Student BYOD Wi-Fi and troubleshooting access issues.
- The school is not responsible for repairing or servicing personal devices.

Student Responsibilities

All students participating in the BYOD programme must use their devices in a manner that supports learning, upholds JBS values, and complies with the school's Acceptable Use Guidelines. The following responsibilities apply whenever a device is used on school premises or during school-related activities.

Daily Readiness:

- Bring the approved device to school each day, unless otherwise instructed by a teacher.
- Ensure the device is fully charged at the start of the school day.
- Keep the device in good working order, free from damage, and ready for learning activities.

Required Software and Updates:

- Install and maintain all school-required software, apps, and security configurations.
- Keep the device's operating system and security software up to date.
- Remove any unauthorised or inappropriate software, apps, or files immediately when instructed by a teacher or IT staff.

Safe Handling and Security

- Store the device in a protective case when not in use.
- Clearly label the device with your full name.
- Do not leave the device unattended in unsecured areas.
- Password-protect the device and keep login credentials secure.

Proudly

tāaleem



Ownership and Liability

- Students are responsible for the maintenance, insurance, and safe keeping of their own devices.
- Any damage, loss, or theft of personal devices is the student's responsibility; the school is not liable for repair or replacement costs.

Parent/Guardian Responsibilities

Parents and guardians play an essential role in ensuring the success of the BYOD programme by providing, maintaining, and supporting their child's responsible and safe use of technology. The following expectations apply for all families participating in BYOD at JBS:

Providing an Approved Device.

- Supply a device that meets the minimum specifications for the student's grade level (see Device Specifications section).
- Ensure the device is fully operational and in good working order before the start of the school year.
- Purchase recommended accessories such as a protective case, screen protector, and headphones to minimise damage and disruption.
- Strongly consider insurance or extended warranty coverage (e.g., AppleCare for iPads) to cover repair or replacement costs, as these can be significant.

Ensuring Required Software and Settings

- Install all school-required software, applications, and security configurations before the device is brought to school.
- Enable safeguarding measures provided by the school or its recommended suppliers (e.g., web filtering, profile management).
- Ensure the device's operating system, applications, and antivirus software are kept up to date.

Supporting Responsible and Safe Use

- Discuss and reinforce the Acceptable Use Guidelines and digital citizenship expectations with your child.
- Monitor your child's device use at home to ensure it aligns with school expectations for responsible, respectful, and safe online behaviour.
- Encourage regular backup of school-work to prevent data loss.

Addressing Repairs, Loss, or Theft

- Take full responsibility for the cost of repairing or replacing the device if it is damaged, lost, or stolen.
- Arrange for timely repairs to minimise disruption to learning.
- Report stolen devices to the police and notify the school immediately.

Acknowledgement and Agreement

- Sign and return the BYOD Agreement Form each academic year before the device is connected to the school network.
- Acknowledge that failure to meet BYOD requirements may result in restricted network access or other measures in line with the school's behaviour management policy.

School Responsibilities

Jumeira Baccalaureate School is committed to ensuring that the BYOD programme supports high-quality teaching and learning while maintaining a safe and secure digital environment. The school will:

Provide a Safe and Secure Digital Learning Environment:

- Maintain a filtered and monitored internet connection in compliance with UAE regulations and JBS safeguarding standards.
- Apply security controls to the Student BYOD Wi-Fi network to protect users from harmful or inappropriate content.
- Implement and enforce measures that prevent unauthorised access to the school's systems and data.

Support Device Integration for Learning:

- Ensure that all teaching and learning platforms (e.g. Microsoft 365, learning management systems, approved educational apps) are compatible with the published device specifications.
- Provide teachers with training and support to effectively integrate technology into classroom learning.
- Offer guidance to students on the appropriate and effective use of their devices for educational purposes.

Provide Limited IT Support for Student Devices:

- Assist with connecting devices to the Student BYOD Wi-Fi network.
- Provide instructions for installing and configuring required software and applications.

- Troubleshoot basic connectivity and access issues.
- Make school-owned loan devices available in the event of short-term device unavailability (e.g., repairs), subject to availability and school policy.

Monitor and Enforce Acceptable Use:

- Monitor network activity and device use when connected to the school network to ensure compliance with the Acceptable Use Guidelines.
- Conduct random device checks where necessary to maintain safeguarding standards.
- Take appropriate disciplinary action in accordance with the JBS Behaviour Management Policy for breaches of the BYOD policy or Acceptable Use Guidelines.
- Communication and Policy Review
- Publish and update the Device Specifications annually to reflect current curriculum and software requirements.
- Communicate BYOD requirements, procedures, and expectations clearly to students, parents, and staff.
- Review the BYOD policy annually to ensure it remains aligned with best practice, safeguarding regulations, and the school's mission and core values.

Acceptable Use Guidelines

JBS recognizes the educational value of personal devices while also promoting healthy, balanced technology habits. To support students' wellbeing and focus, the following acceptable-use expectations apply to all BYOD users; the policy ensures devices are used purposefully to support teaching and learning, protect instructional time and classroom focus, reduce distraction and addictive behaviours, safeguard school networks and student data, and promote responsible digital citizenship. It provides clear expectations around permitted activities, sound, network connections, reporting and compliance enabling the school to manage technology effectively and uphold JBS's mission, the IB philosophy, and our Core Values of Responsibility, Respect, Resourcefulness and Resilience.

Acceptable Use (Devices)

The use of technology at Jumeira Baccalaureate School is a privilege, not a right. Students are expected to use their devices in ways that enhance learning, uphold the school's core values; Responsibility, Respect, Resourcefulness, Resilience and comply with all school, UAE, and international laws.

The following guidelines apply to all use of personal devices on school premises or during school-related activities:

Educational Purpose:

- Use your device only for activities directly related to learning, as directed by your teachers.
- Access only school-approved websites, applications, and online resources during class time.
- Keep personal use (e.g., messaging, entertainment, gaming) outside of instructional time unless approved for a specific learning activity.

Respect and Digital Citizenship:

- Communicate respectfully and responsibly with peers, teachers, and the wider school community online.
- Do not use language or share images that are offensive, discriminatory, harassing, or inappropriate.
- Protect your own privacy and the privacy of others; do not share personal information, passwords, or photos without permission.

Network and System Security:

- Connect only to the Student BYOD Wi-Fi; do not use personal hotspots or mobile data on campus.
- Do not use VPNs, proxies, or other tools to bypass school security and content filters.
- Do not attempt to hack, access, or modify school systems, networks, or other people's files.
- Report any security concerns or suspicious activity to IT immediately.

Content Standards:

- Do not access, download, store, or share any content that is illegal, offensive, pornographic, violent, extremist, or otherwise inappropriate for a school environment.
- Do not engage in file-sharing of copyrighted material without permission.
- Respect intellectual property by crediting sources and following copyright laws.

Device Management:

- Keep your device secure, password-protected, and in a protective case.
- Do not install unapproved software or apps on your device for use at school.
- Keep sound muted unless required for learning and approved by a teacher.
- Follow teacher instructions for when to close devices, switch off screens, or store them.

Acceptable Use (Digital Wellbeing)

JBS recognises the educational value of personal devices while also promoting healthy, balanced technology habits.

To support students' wellbeing and focus, the following acceptable-use expectations apply to all BYOD users:

Device Use:

- Devices may only be used for learning during lessons unless a teacher explicitly permits personal use for wellbeing, collaboration, or approved school activities.
- Students will switch devices to "classroom/focus" mode (Do Not Disturb, announcements off) when asked by staff.

Device-free Periods:

- All students must put devices away during registration, assemblies, break/lunch times, and during unstructured social time unless supervised activity requires them.
- No device use is allowed in bathrooms or changing rooms.

Screen Time Limits (school hours):

- Teachers will design lessons that include regular device breaks and use a mix of digital and non-digital activities.
- Primary classrooms will use short, teacher-timed device sessions; secondary students will follow negotiated classroom agreements that balance online/offline learning.

Notification Management:

- Students are expected to disable non-essential notifications during school hours and at agreed quiet times to reduce distraction.

Restricted Apps & Sites:

- Entertainment and social apps that are not required for learning should not be used on the school network during lesson time.
- The school may restrict access to high-risk or highly addictive sites during school hours.

Evening & Homework Guidance:

- Students and families are encouraged to follow recommended evening device routines (e.g., device free 30-60 minutes before bedtime) to support sleep hygiene.
- Teachers will set homework expectations that avoid excessive screen time where possible.

Digital Wellbeing Education:

- All students will receive age-appropriate lessons on healthy device use, self-regulation strategies, and recognising problematic use.

Support & Consequences:

- Staff will use a restorative approach for breaches
- *(reminder → restorative conversation → parent/guardian contact → temporary loss of BYOD privileges for repeated breaches).*
- Persistent concerns will trigger referral to wellbeing or counselling services.

Monitoring and Consequences

All activity on the Student BYOD Wi-Fi is monitored. The school reserves the right to inspect student devices connected to the school network.

Breaches of this guide will result in consequences under the JBS Behaviour Management Policy and may include:

- Temporary or permanent loss of network access
- Confiscation of the device until collected by a parent/guardian
- Additional disciplinary measures
- Referral to law enforcement for serious offences

Prohibited Activities

To protect the safety, integrity, and effectiveness of our digital learning environment, the following activities are strictly prohibited when using personal or school-owned devices on JBS premises or during school-related activities:

Online Activities:

- Gaming, streaming, or using social media during lessons unless approved for learning.
- Taking photos, videos, or recordings without the consent of all parties and teacher approval.
- Cyberbullying or engaging in any online behaviour that causes harm to others.
- Participating in scams, phishing, credit card fraud, or any illegal online activity.
- Using anonymous or false identities for communication.
- Connecting unapproved storage devices or peripherals to the school network.

Bypassing or Tampering with Security:

- Using VPNs, proxy servers, or other tools to bypass the school's network filters or monitoring systems.
- Attempting to hack, access, or modify school systems, networks, or other users' accounts and files.
- Installing unauthorised software, apps, or extensions that compromise security.

Accessing or Sharing Inappropriate Content:

- Viewing, downloading, storing, or distributing content that is illegal, pornographic, violent, extremist, discriminatory, or otherwise inappropriate for a school setting.
- Possessing or sharing material that promotes hate speech, harassment, or abuse.

Misuse of Communication Tools:

- Sending or posting messages, images, or videos that are offensive, threatening, harassing, or discriminatory.

- Using anonymous or false identities to communicate.
- Engaging in cyberbullying or any form of online harassment.

Personal Use During Instruction:

- Playing games, streaming entertainment, or using social media during lessons unless explicitly authorised for learning purposes.
- Using messaging services (e.g., WhatsApp, Snapchat, Instagram DMs) during instructional time without teacher approval.

Recording and Photography Without Consent:

- Taking photos, videos, or audio recordings of students, staff, or visitors without their consent and the approval of a teacher.
- Sharing any recordings or images without permission from all parties involved.

Illegal or Unethical Activities:

- Engaging in fraud, phishing, or any other illegal online activity.
- Participating in copyright infringement by downloading or sharing copyrighted material without permission.
- Using the school's network for financial gain, advertising, or unauthorised commercial activity.

Unauthorized Device Connections:

- Connecting unapproved external storage devices, peripherals, or equipment to the school's network.
- Using personal hotspots or mobile data on campus to bypass school systems.

Damage or Disruption:

- Deliberately introducing viruses, malware, or other harmful programs to school or personal devices.
- Participating in any activity that disrupts the learning environment, damages hardware/software, or interferes with the school's digital infrastructure.

Device Inspection & Confiscation

To ensure compliance with the JBS BYOD policy, Acceptable Use Guidelines, and safeguarding standards, the school reserves the right to inspect and, when necessary, confiscate student devices.

Device Inspection:

- Devices connected to the Student BYOD Wi-Fi or used on school premises are subject to inspection at any time.
- Inspections may be random or targeted when there is reasonable cause to suspect:
 - Violation of the BYOD policy or Acceptable Use

- Access to or possession of inappropriate or prohibited material
- Attempts to bypass network security or filters
- Engagement in illegal or unsafe activities
- Inspections will be conducted by authorised staff in a manner that respects student privacy while upholding safeguarding requirements.
- Students must cooperate fully with staff during an inspection, including unlocking the device and navigating to requested files or applications.

Device Confiscation:

- A device may be confiscated when:
 - Device is used in violation of the BYOD policy or Acceptable Use
 - Device contains prohibited content or applications
 - Device is used to disrupt the learning environment
 - Device is involved in a safeguarding or disciplinary investigation
- Confiscated devices will be stored securely until they are collected by a parent or guardian.
- Depending on the severity of the violation, confiscation may be temporary (returned the same day) or extended until the matter is resolved.

The school will not be responsible for damage or loss while the device is in confiscation storage.

Consequences

Device confiscation may be accompanied by additional disciplinary actions in line with the JBS Behaviour Management Policy. Repeated offences may result in:

- Suspension of BYOD privileges
- Permanent loss of access to the Student BYOD Wi-Fi
- Further sanctions determined by the school leadership
- Serious breaches involving illegal activity or safeguarding risks may be referred to law enforcement or relevant UAE authorities.

Security, Safety, and Liability

Jumeira Baccalaureate School is committed to providing a secure and safe digital learning environment. Students and families are responsible for ensuring that personal devices meet security standards and are used in a way that protects all members of the school community.

Device Security:

Proudly
tdaleem



CIS
ACCREDITED



AFS
SCHOOL OF
CHARACTER

Pearson
BTEC

The
Alliance for
Sustainable
Schools

مدرسة جميرا للبكالوريا
JUMEIRA
BACCALAUREATE
School

- All devices must be password-protected and secured with a PIN, passcode, or biometric lock.
- Antivirus or endpoint protection software must be installed and kept up to date on all laptops.
- Devices must be configured with school-approved security profiles or safeguarding settings before connecting to the Student BYOD Wi-Fi.
- Students must not disable or alter security settings, filters, or monitoring tools installed by the school or recommended suppliers.

Online Safety:

- Students must always follow the Acceptable Use Guidelines and digital citizenship Guidelines.
- The school's internet connection is filtered and monitored to prevent access to harmful or inappropriate material; students must not attempt to bypass these protections (e.g., using VPNs or proxy servers).
- Personal data (such as full name, address, phone number, or passwords) should never be shared online without permission from a parent/guardian and teacher.

Safeguarding:

- The school reserves the right to inspect devices when safeguarding concerns are raised or policy breaches are suspected.
- Any online behaviour that poses a risk to the safety, wellbeing, or reputation of a student or the school will be treated as a serious disciplinary matter.
- Incidents involving illegal content or activity will be referred to UAE authorities in accordance with the law.

Liability:

- Students and families are responsible for the care, maintenance, insurance, and security of personal devices.
- The school will not be held liable for the loss, theft, or damage of personal devices on school property or during school-related activities.
- Repair or replacement costs are the sole responsibility of the student's family.
- The school may provide loan devices in emergencies, subject to availability and school policy, but is not obliged to replace or permanently substitute personal devices.

Reporting

- Lost or stolen devices must be reported immediately to the school office and, if necessary, to the Dubai Police.
- Any suspected security breach, virus infection, or exposure to inappropriate material must be reported to IT staff without delay.

Misuse and Disciplinary Action

The BYOD programme is designed to enhance learning, not disrupt it. Misuse of personal devices will be addressed in line with the JBS Whole School Behaviour Management Policy and the school's safeguarding commitments.

Definition of Misuse

Misuse includes, but is not limited to:

- Breaching the Acceptable Use Guide or Prohibited Activities list.
- Accessing or storing inappropriate content.
- Using the device in a way that disrupts learning.
- Attempting to bypass school security (e.g., VPNs, proxies, hacking).
- Engaging in online harassment, cyberbullying, or sharing offensive material.
- Ignoring staff instructions regarding device use.
- Refusing to cooperate with device inspections.

Behaviour Levels and Consequences

Misuse will be categorised using the JBS Behaviour Management Policy levels:

Level 3 Behaviours:

- Repeated inappropriate device use in lessons.
- Accessing unapproved websites.
- Minor defiance.
- Inappropriate language online.

Possible Consequences:

- Verbal warning and restorative conversation.
- Confiscation of the device for the remainder of the lesson or day.
- Parental contact.
- Recording on CPOMS.

Level 4 Behaviours:

- Repeated Level 3 offences.
- Serious breaches such as cyberbullying, harassment, bypassing security systems, accessing or sharing explicit/illegal content, or using a device to commit a safeguarding offence.

Possible Consequences:

- Immediate confiscation of the device.
- Suspension of BYOD privileges for a defined period or permanently.
- Formal written warning letter filed with the KHDA.
- Possible fixed-term exclusion in line with KHDA guidance.
- Referral to law enforcement for illegal activities.

Confiscation Procedures

- Devices confiscated for misuse will be stored securely and may only be collected by a parent or guardian.
- For repeated or severe incidents, the device may be held until a formal meeting is conducted with parents and school leadership.

Restorative Approach

Where appropriate, students will complete a reflection form to consider the impact of their actions, guided by the 4R's: Responsibility, Respect, Resourcefulness, and Resilience.

Restorative conversations may be used to rebuild trust and reinforce positive digital behaviours.

Permanent Loss of Privileges

- Students who receive three KHDA-filed warning letters for Level 4 behaviour will be asked to transfer to another school, in accordance with the Behaviour Management Policy.
- BYOD access may be withdrawn permanently if misuse poses a continuing risk to safety, learning, or the school's digital environment.

Agreement and Acknowledgement

Participation in the JBS BYOD programme is a privilege that requires a shared commitment between the student, parent/guardian, and the school. Before any personal device can be connected to the Student BYOD Wi-Fi or used in lessons, the following agreement must be read, understood, and signed by both the student and their parent/guardian.

By signing this agreement, all parties agree to the following:

Student Commitment

I understand and agree to:

- Bring a device that meets the JBS Device Specifications for my grade level.
- Use my device in accordance with the BYOD Policy, Acceptable Use Guide, and JBS Behaviour Management Policy.
- Keep my device secure, fully charged, and in good working order each day.

Proudly

táaleem



- Follow teacher instructions for device use in class.
- Respect the privacy, safety, and learning of others.
- Not engage in any Prohibited Activities outlined in the policy.
- Report any technical, security, or safeguarding concerns immediately to a teacher or the IT Department.
- Cooperate fully with any device inspection by authorized staff.

Student Commitment Signatures

Electronic signatures collected

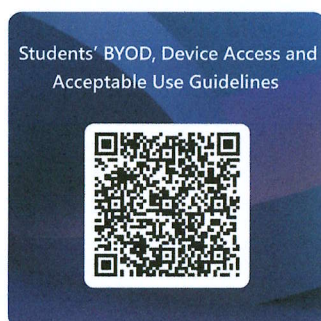
Parent/Guardian Commitment

I understand and agree to:

- Provide my child with an approved device that meets JBS specifications and ensure it is maintained in good working condition.
- Purchase recommended protection (e.g., insurance or extended warranty such as AppleCare) to cover repair or replacement costs, understanding the school is not responsible for loss, theft, or damage.
- Ensure all required software, applications, and safeguarding settings are installed and kept up to date.
- Discuss responsible device use with my child and support the school's Acceptable Use expectations.
- Respond promptly to school communication regarding device misuse or policy breaches.
- Accept that misuse may result in temporary or permanent loss of BYOD privileges.

Parent/Guardian Commitment Signatures

Scan or click the link below to sign the form.



<https://forms.office.com/r/svMnbgfJvE>

Proudly
tāaleem



CIS
ACCREDITED



IB School
CHARACTER

Pearson
BTEC

The Alliance for
Sustainable
Schools

مدرسة جميرا للبكالوريا
JUMEIRA
BACCALAUREATE
School

School Commitment

JBS agrees to:

- Provide a safe, filtered, and monitored digital environment for learning. □
- Support students in connecting approved devices to the school network.
- Offer guidance and training for responsible and effective technology use.
- Monitor compliance with the BYOD policy and take appropriate action to maintain a safe learning environment.
- Communicate clearly with students and parents regarding expectations, incidents, and consequences.

