

BYOD & Personal Device Policy

Policy Owner	SLT
Approved by	Ms Sapna Changrani (Head of School)
Review Date	July 2026
Next Review Due	July 2027
Circulation	All Staff, Students, Parents; School Website; KHDA Inspection File

1. PURPOSE

This policy governs the possession and use of all personal electronic devices — including mobile phones, tablets, laptops, smartwatches, and earphones — by students at Dubai Scholars Private School during the school day, on school transport, and at school-sponsored activities. It is designed to protect the safety, wellbeing, and privacy of all members of the school community; prevent disruption to learning; ensure compliance with UAE law; and reflect the school's commitment to responsible digital citizenship.

2. MOBILE PHONE PROHIBITION -



MOBILE PHONES ARE NOT PERMITTED FOR USE AT SCHOOL

With effect from the start of Academic Year 2026-27, students are not permitted to use mobile phones at any time during the school day, including during breaks, lunch, and transition between lessons.

All mobile phones must be stored in a school-issued locked pouch (DISCONNECT) from the moment the student arrives on school premises until dismissal.

Locked pouches must be purchased from the school at the start of the academic year. The cost will be communicated to parents before the start of the term.

Students retain physical possession of their locked pouch at all times; it is unlocked only at designated unlocking stations upon exit from the school at dismissal.

- This rule applies on all school days from arrival to dismissal, including before-school and after-school activities held on the school premises
- Students on school transport must store their phone in the locked pouch before boarding and may not access it during the journey
- Students who require access to their phone for a verified medical reason (e.g., monitoring a health device) must provide written medical evidence to the school nurse; an individual exception plan will be agreed in writing with the Head of School
- Parents wishing to contact their child during the school day must call the school office; the school will relay urgent messages to students

3. PERMITTED DEVICES – LAPTOPS AND TABLETS (Year 3 upwards)

Where the school requires or permits students to bring a personal laptop or tablet for educational use, the following rules apply. The school provides suitable technology for learning; teachers may permit, but will not require, use of a personal device where a school device is not available.

3.1 Permitted Use

- Personal laptops and tablets may be used only for school-prescribed educational tasks as directed by the teacher
- Only apps, tools, and platforms prescribed or approved by the school are permitted on devices brought onto school premises; see Section 4 for the approved and prohibited app list
- Device use is permitted only during lessons when explicitly instructed by the teacher; devices must be closed and stored at all other times unless a teacher specifies otherwise
- All personal devices connecting to the school network must comply with the school's Acceptable Use Policy and network access rules. Use of VPN is not permitted.

3.2 Device Requirements

- Devices must be fully charged before arriving at school; charging on school premises is not guaranteed
- Devices must have up-to-date operating systems and security software; the school is not responsible for maintaining or troubleshooting personal devices
- Students must not share their device or login credentials with other students

4. PERMITTED AND PROHIBITED APPLICATIONS

APP POLICY – SCHOOL-PRESCRIBED APPS ONLY

Personal devices brought to school may only have apps and platforms that are prescribed or approved by the school installed and active during the school day.

Any non-school app found in use on a personal device on school premises is a violation of this policy and will result in the consequences set out in Section 8.

Application / Platform	Status at Dubai Scholars
School-prescribed learning platforms	✓ Permitted — as directed by teacher (e.g., Toddle Student App, Achieve 3000, Non-Arab platform and other subject-specific tools approved by the school)
iMessage / SMS with parents during school	✗ Strictly prohibited during lessons; parent communication Only via the school office is permitted
Social media platforms	✗ Prohibited at all times on school premises (Instagram, TikTok, Snapchat, X/Twitter, Facebook, and equivalents)
Google Chat, Google Meet (non-school)	✗ Prohibited — personal Google accounts and non-school communication platforms are not permitted
WhatsApp and other messaging apps	✗ Prohibited — no third-party messaging apps permitted during school hours on school premises
Gaming apps and entertainment platforms	✗ Prohibited — gaming apps, streaming services (YouTube, Netflix, Spotify), and entertainment apps are not permitted at any time on school premises
VPN applications	✗ Strictly prohibited — use of VPNs is illegal under UAE law (TDRA); any student found using a VPN faces immediate referral to the Head of School and may face legal consequences
Unauthorised AI tools	✗ Prohibited unless specifically approved by a teacher for a

Application / Platform	Status at Dubai Scholars
	defined task; use of AI tools to complete assessed work without disclosure is treated as academic dishonesty

5. PRIVACY AND RECORDING

Under UAE Federal Law No. 5 of 2012 (Cybercrime Law) and Wadeema's Law, the recording, photographing, or filming of other individuals without their consent, and the sharing of such material, is a criminal offence. The following rules apply at all times on school premises, on school transport, and at school-sponsored activities:

- Students must not record, photograph, or film other students, staff, or visitors without their explicit consent
- Students must not share, upload, or post any images or videos taken at school on any platform, including social media, messaging apps, or cloud storage, without the consent of all individuals depicted
- Recording, photographing, or filming in changing rooms, toilets, health offices, prayer rooms, or any space with a reasonable expectation of privacy is strictly prohibited and will be treated as a serious safeguarding matter
- School events and activities — including sports days, performances, and assemblies — are not public arenas; the same consent rules apply
- Any recording obtained in violation of this policy must be deleted immediately upon instruction from a member of staff; failure to comply is a further violation

6. ACADEMIC INTEGRITY

- No personal device may be used during any assessed task, test, or examination unless explicitly permitted in writing by the Examinations Officer for a specific student with verified access arrangements
- Having a device visible or within reach during an assessment, even if switched off, may be treated as an attempt to cheat and will be handled under the school's Academic Integrity Policy
- The use of any audible or wireless transmission during a test or examination will result in immediate removal from the assessment room and cancellation of the paper; the matter will be referred to the Phase Head and parents notified
- Use of AI tools or any digital resource to complete assessed work without explicit teacher permission and disclosure constitutes academic dishonesty and is subject to the consequences set out in the Academic Integrity Policy

7. RESPONSIBILITY FOR PERSONAL PROPERTY

- Students who bring any personal device to school do so entirely at their own risk; the school, its staff, and its employees accept no liability for the loss, theft, damage, destruction, or misuse of any personal device on school premises, on transport, or at school-sponsored activities
- Personal devices on cellular networks are not subject to the school's internet filters; responsibility for appropriate internet use via mobile data rests with the student and parent
- School staff will not store, safeguard, repair, or troubleshoot any student's personal device
- Confiscated devices will be held securely by the Phase Head and returned in accordance with Section 8; the school accepts no liability for a device during the confiscation period

8. VIOLATIONS AND CONSEQUENCES



CONFISCATION RULE – 2026-27

Any device found in use in violation of this policy — including a mobile phone found outside its locked pouch, a device with prohibited apps open, or a device used for unauthorised communication or content — will be confiscated immediately by the relevant Phase Head.

The period of confiscation will be determined by the Phase Head based on the nature and severity of the violation. The device will be returned to the parent or guardian in person; it will not be returned directly to the student.

Violation Level	Consequence
Level 1 – Minor violation	Phone found outside locked pouch; non-school app open but no harmful content. Consequence: Device confiscated by Phase Head; parent informed; returned to parent/student after period (a maximum of 3 days) determined by Phase Head; recorded on student file.
Level 2 – Moderate violation	Unauthorised communication during school hours; gaming or entertainment app use; device use during a lesson without permission. Consequence: Device confiscated for upto a week; written warning on the Toddle behaviour module.
Level 3 – Serious violation	Accessing inappropriate content; cyberbullying; unauthorised recording of students or staff; use of VPN; device use during an assessed task. Consequence: Device confiscated; referred to Head of School; parents required to attend; suspension possible; matter referred to DSL if safeguarding concern identified; possible referral to KHDA or UAE authorities. Written warning on Toddle and Behaviour policy ramifications will be applicable. Parents will be called in for a meeting with Phase Head and relevant parties.
Level 4 – Severe / criminal violation	Creating, sharing, or distributing inappropriate or illegal content; recording in private spaces; violations of UAE Cybercrime Law. Consequence: Immediate suspension; referral to police / DCPA as required by UAE law; possible expulsion; school has a legal obligation to report. Written warning on Toddle and Behaviour policy ramifications will be applicable. Parents will be called in for a meeting with Head of School and relevant staff.

Multiple violations at any level may result in escalation to the next level. All violations are recorded on the student's file on Toddle. Parents will be notified of all confiscations and Level 2 violations and above.

9. DIGITAL CITIZENSHIP AND EDUCATION

- The school embeds digital citizenship education across the curriculum; students are taught responsible, ethical, and safe use of technology as part of their personal development
- Age-appropriate online safety sessions are delivered to all year groups at least once per academic year, covering topics including cyberbullying, privacy, consent, and UAE legal obligations
- Parents receive guidance on supporting responsible device use at home, including monitoring tools, age-appropriate content filters, and the school's expectations for home device use

10. PARENT AND STUDENT AGREEMENT

This policy takes effect at the start of Academic Year 2026-27. Before the first day of term, all parents and students in Years 3 and above are required to sign and return the Dubai Scholars BYOD & Personal Device Acceptable Use Agreement, confirming they have read and understood this policy. Failure to return the signed agreement does not exempt a student from compliance with this policy.

- Signed agreements are held on the student's file and are available to KHDA inspectors on request
- Locked pouches must be purchased from the school office before or on the first day of term; the cost and payment process will be communicated to parents in the pre-term letter

11. MONITORING AND REVIEW

- Compliance with this policy is monitored daily by Phase Heads, class teachers, and duty supervisors; all violations are logged centrally by the Head of School's office
- The policy is reviewed annually each July, or earlier if a significant incident, new UAE legislation, KHDA guidance, or changes to available technology require an interim review
- Anonymised incident data is reported to the Board of Governors annually

12. POST-16 (SIXTH FORM) PROVISIONS

The following provisions apply specifically to students in Years 12 and 13 and recognise the increased independence and academic responsibilities associated with post-16 education.

- **Mobile Phone Storage and Use:** Post-16 students are required to secure their mobile phones in the school's designated locked pouch system (DISCONNECT) upon arrival, in accordance with Section 2. Access to mobile phones may be permitted within designated Sixth Form study areas (Student Hub) during free periods, independent study sessions, and lunch breaks for academic purposes and personal organisation only. This exception does not extend to lessons, transitions between classes, assemblies, examinations, or any other areas of the school.
- **Use of Laptops and Tablets for Independent Study:** In addition to the provisions outlined in Section 3.1, Post-16 students may use personal laptops or tablets during supervised independent study periods in Student Hub. Such use may include coursework completion, research, revision, note-taking, and access to approved educational platforms and resources.
- **University, College, and Career Applications:** Access to university and college application systems, including UCAS, Common App, scholarship portals, and related email correspondence, is recognized as an authorized educational activity. Students may engage with these platforms during independent study periods and within the Student Hub under appropriate supervision.
- **Coursework and Examination Requirements:** Where examination boards (e.g., Pearson Edexcel or Cambridge) require the completion of coursework, internal assessments, or computer-based assessment components using personal devices, such use shall be permitted in accordance with the guidance and supervision arrangements established by the school.
- **Smartwatches:** Smartwatches devices may be worn for legitimate purposes such as timekeeping, fitness tracking, and calendar or examination reminders. However, all communication, messaging, social media, internet access, and notification functions must remain disabled during the school day and throughout assessments. Any misuse involving unauthorized communication, recording, or access to restricted content will be treated as a breach of this policy and managed in accordance with the school's behaviour procedure.

13. POLICY REVIEW

 This policy will be reviewed annually, or sooner if required, to reflect operational needs, changes in legislation, or updated guidance from the KHDA.