FOUNDED 1900
THE ENGLISH SCHOOL
A SECOND CENTURY OF EXCELLENCE

Bring Your Own Device (BYOD) Policy

The English School

Person responsible for policy	Stavroula Neokleous (Assistant Head) Harris Evangelou (Assistant Digital Lead)
Ratified by	The Board of Management
Version	September 2026 (v1)
Date Approved	2nd November 2026
Review Period	1 year
Next Review date	September 2027
Companion Document	Digital Wellbeing Framework

Contents

Introduction 1
Technology and Learning at The English School 1
BYOD at The English School: Scope and Purpose 1
How Technology Is Used Across Departments 2
Subject-Specific Digital Tools and Resources 2
Responsibilities 3
The School 3
Teachers 3
Parents and Guardians 4
Students 4
Academic Integrity and the Use of AI 4
Safeguarding and Network Use 5
Device Requirements 5
Screen Time and Device Use in Lessons 5
Homework and Assignments 5
Assessments and Examinations 5
Misuse and Sanctions 6
Related Policies 7
Appendix A: Parent and Student Frequently Asked Questions (FAQ) 8
Appendix B: Parent and Student Agreement Form 12
Student Responsibilities 12
Parent and Guardian Responsibilities 12
School Responsibilities 12

Introduction

We live in a world shaped by digital technology. From the sciences to the arts, from communication to creative design, technology has become an inseparable part of how people learn, work, and contribute to society. The ability to use digital tools with confidence, purpose, and critical awareness is no longer a supplementary skill, it is a foundational one. The English School recognises this reality and embraces it as an opportunity to deepen and enrich the education we offer.

The Bring Your Own Device (BYOD) Policy directs the use of personally owned digital devices (tablets) within the School. Rather than viewing technology as a complication to be managed, the School views it as a resource to be cultivated and one that, when used thoughtfully and purposefully, enhances the quality of teaching and learning for every student.

This Policy sets out the rules, responsibilities, and sanctions that govern device use at The English School. It is accompanied by a separate Digital Wellbeing Framework, which explains the reasoning behind the School's approach to screen time, focus, and healthy digital habits. Where a rule in this Policy relates to student wellbeing, a cross-reference to the Digital Wellbeing Framework is provided.

Technology and Learning at The English School

At The English School, academic excellence and whole-person development have always gone hand in hand. Technology, when integrated with intention and professional judgement, is a powerful enabler of both. Digital tools can make abstract concepts tangible, support students who learn in different ways, allow for rapid feedback, and open windows onto resources and perspectives far beyond the classroom.

Research consistently demonstrates that purposeful use of technology in education deepens engagement, strengthens critical thinking, and prepares young people for higher education and the professional world. Our students are preparing for careers in fields that do not yet fully exist, and the habits of mind they develop around digital tools, like curiosity, judgment, responsibility and adaptability are every bit as important as the content knowledge they acquire.

The School is committed to building a culture where technology serves learning, not the other way around. This means teachers making deliberate, pedagogically grounded decisions about when and how to use devices in lessons; students approaching digital tools with independence and integrity; and parents and guardians reinforcing the same values at home. Together, these shared commitments make BYOD not simply a logistical arrangement but an expression of the School's educational vision.

BYOD at The English School: Scope and Purpose

The School operates a Bring Your Own Device environment in which students bring their own tablets to use for educational purposes during the school day. At present, bringing a device is compulsory for students in years 1-4 and optional for students in years 5-7. All devices used on school premises are privately owned by students and are maintained externally from the School. The School does not provide technical support or repairs and accepts no responsibility for their loss, theft, damage, or malfunction.

The purpose of BYOD is not to replace traditional learning but to extend it. Devices give students access to collaborative platforms, interactive resources, and subject-specific software that would otherwise be unavailable in a conventional classroom setting. They enable students to develop the practical digital literacy that universities and employers expect, while remaining firmly anchored in the School's academic values of rigour, integrity, and independent thought.

Personal devices are for use within the classroom environment only, under the direction of a teacher. Devices may not be used in corridors, communal areas, or during breaks. This expectation supports student wellbeing; see the Digital Wellbeing Framework for the full rationale.

This policy applies to and must be adhered to by all students, teachers, parents, and guardians. It directs the use of personal digital devices in all School environments and during all school-related activities.

Use of a personal device on school premises is a privilege, not a right, and the School reserves the right to withdraw that privilege where the terms of this policy are not observed.

How Technology Is Used Across Departments

At The English School, digital learning is embedded across all subject areas and year groups. The core technology platform used throughout the school is Microsoft 365, with Microsoft Teams, OneNote, OneDrive, Outlook, Forms, Word, PowerPoint and Excel supporting communication, organisation, collaboration, assessment and learning activities in every department. This common platform ensures a consistent experience for students and enables them to access learning resources, submit work, collaborate with peers and communicate with teachers regardless of subject.

Alongside Microsoft 365, departments make use of a range of carefully selected subject-specific applications, online platforms and subscription services that support particular curriculum requirements. All device use in lessons, including use of these platforms, is guided by the School's approach to screen time set out in the Screen Time and Device Use section below.

Subject-Specific Digital Tools and Resources

Department	Additional Platforms & Tools	Notable Use in Lessons
Biology	e-Chalk, Save My Exams, Exam Wizard	Data analysis, revision activities, collaborative note-taking and examination preparation
Chemistry	ChemGuide, e-Chalk	Structured revision, independent study and examination preparation
Computer Science	ChatGPT, coding environments and development tools	Coding practice, algorithm design, computational thinking and software development
Design & Technology	Fusion 360, Blender, LightBurn, Inkscape, Procreate, Sharp3D	CAD/CAM design, digital fabrication, prototyping and industry-standard design practices
English	Reading Plus, Padlet, Quizlet, Canva	Reading development, vocabulary building, digital annotation, collaboration and creative presentation
Geography	Google Earth, Google Maps	Spatial enquiry, fieldwork support, mapping skills and geographical analysis
Greek	Kahoot!, Quizlet, Wordwall, Digital Ministry Textbooks	Vocabulary development, language practice, formative assessment and independent study

Department	Additional Platforms & Tools	Notable Use in Lessons
History	Canva, Blooket	Source analysis, research projects, revision activities and student presentations
Mathematics	Collins Hub, Pearson ActiveLearn, Desmos, CODAP, Dr Frost Maths	Graphical exploration, statistical analysis, adaptive practice and examination preparation
Modern Foreign Languages	Blooket, LanguageNut, Pearson Platform	Vocabulary acquisition, listening and speaking practice, revision and independent learning
Music	BandLab, GarageBand, MuseScore	Digital composition, recording, music production, notation and performance development
Physical Education	Boost	Activity tracking, performance monitoring, fitness assessment and student engagement
Physics	Kahoot!, Save My Exams, Digital Textbooks	Revision activities, formative assessment, independent study and examination preparation
Turkish	Subject-specific digital resources and online reference materials	Presentation tasks, language development, research activities and written work

Responsibilities

The School

The School will provide a secure, filtered Wi-Fi network for student and staff use during the school day. It will implement appropriate monitoring and internet filtering to promote a safe online environment and will ensure that teachers are equipped with the guidance, training, and support necessary to integrate technology effectively into their teaching. The School will communicate clear expectations to students and parents, review this policy annually, and take appropriate action in cases of misuse.

Teachers

Teachers are at the heart of purposeful technology use. They are responsible for deciding when and how devices are used within their lessons, ensuring that such use is purposeful, supervised, and aligned with learning objectives. Before permitting device use, teachers will ensure that students understand the expectations for that particular activity. They will provide clear guidance on which platforms or tools are to be used, intervene promptly if devices are being used inappropriately, and record incidents of misuse in the School's incident management system.

Teachers will remain conscious of the amount of time devices are used during their lessons, ensuring that device use is purposeful and balanced with other learning activities (see Screen Time and Device Use in Lessons). When setting homework via Teams, teachers will state if an assignment requires a significant amount of screen time. Teachers are not expected to check or respond to student or parent messages after 18:00 on school days.

Teachers will continue developing their own digital literacy, exploring how emerging tools and platforms can further enrich learning in their subjects. The School actively supports professional development in this area and welcomes teacher-led innovation.

Parents and Guardians

Parents and guardians play an essential role in making the BYOD environment work well. They are responsible for providing and maintaining any personal device brought to school, ensuring it is suitable for educational use, fully charged, and protected with appropriate security settings.

Parents and guardians are responsible for the applications, software, and social media platforms installed on their child's device, and should ensure that notifications from these are disabled during the school day to minimise disruption. Devices brought to school must not be fitted with an eSIM, SIM card, or any other means of independently connecting to external mobile networks; devices should connect to the internet only via the School's authorised Wi-Fi.

Parents are asked to support the values of this policy at home, encouraging their child to use technology responsibly, monitoring use outside school hours, and discussing with their child the expectations set out in this document.

Students

Students are expected to use their devices as learning tools and to treat that privilege with maturity and respect. This means using devices only when a teacher has given permission, remaining focused on the educational task at hand, connecting exclusively to the School's authorised Wi-Fi network, and storing devices safely when not in use.

Students must set their device to Do Not Disturb mode for the duration of the school day, and must use their device only within the classroom environment, as directed by a teacher. Devices must not be used in corridors, communal areas, or during breaks.

Students must not attempt to access, store, or share inappropriate content, bypass School network controls, or use devices in ways that disrupt the learning of others. Students are also expected to take care of their own device and to understand that the School bears no responsibility for any loss or damage. Security settings should be maintained, and personal passwords and login credentials must not be shared with others.

Academic Integrity and the Use of AI

The School's commitment to academic excellence rests on a foundation of integrity. Devices and the digital tools they provide access to, including AI-assisted platforms, are resources to support learning, not substitutes for a student's own thinking. Students must ensure that all work submitted for assessment genuinely reflects their own understanding, analysis, and creativity. The use of AI tools to generate, complete, or substantially compose assessed work, without explicit permission and appropriate acknowledgement, constitutes academic malpractice and will be treated accordingly.

Where AI tools are used in a learning context, for example, to explore ideas, receive feedback on drafts, or practise language skills, this is entirely consistent with the School's values, provided the student remains the author of their own thinking and the use is transparent. This policy should be read in conjunction with the School's Use of AI Tools Policy, which sets out in full the expectations and guidelines for the appropriate use of AI across all subject areas.

Ensuring that AI tools are used safely and ethically is as much a staff responsibility as a student one. Teachers receive training on the appropriate use of AI platforms in an educational setting, including how to safeguard students' personal data, avoid inputting identifiable student information into external AI tools, and select platforms that meet the School's data protection standards. This training is reviewed and updated as AI platforms and associated risks evolve,

ensuring that the integration of AI into teaching and learning is never allowed to come at the expense of student privacy or safeguarding.

Safeguarding and Network Use

The School takes its safeguarding responsibilities very seriously. All students and staff must connect personal devices to the School's authorised Wi-Fi network when accessing the internet on school premises. The use of personal hotspots and mobile data connections is strictly prohibited. The School's network applies internet filtering designed to promote safe and appropriate online behaviour, and the School reserves the right to monitor network activity where necessary for safeguarding, security, or operational purposes.

Where device use raises a safeguarding concern, including the discovery of inappropriate imagery, harmful communications, or contact with unknown external individuals, the School's Designated Safeguarding Lead will be notified immediately and the appropriate procedures followed in accordance with the Safeguarding and Child Protection Policy.

Device Requirements

All devices brought to school must be fully charged before arrival, protected with a password, PIN, or biometric lock, and suitable for educational use. Devices must not be fitted with an eSIM, SIM card, or any other means of independently connecting to external mobile networks. Students are encouraged to use a protective case to guard against accidental damage, to keep their device's operating system and applications up to date, and to back up their work regularly. The School accepts no responsibility for technical faults, data loss, or any other device-related issues that arise during the school day.

Students should also ensure that any subject-specific applications required by their department are installed and kept up to date; details of these will be communicated by the relevant teacher at the start of the course.

Screen Time and Device Use in Lessons

The following rules apply to device use during lessons and are enforced by teachers. The reasoning behind these rules is set out in the Digital Wellbeing Framework.

- Teachers are conscious of the amount of time devices are used during lessons and ensure that device use is purposeful, proportionate and balanced with other forms of learning.
- Some lessons may naturally involve more extended device use, for example Computer Science or project-based lessons in other subjects.
- Devices must be set to Do Not Disturb mode for the duration of the school day.
- Devices are for use within the classroom environment only, and may not be used in corridors, communal areas, or during breaks.

Homework and Assignments

- Where a homework assignment requires a significant amount of screen time, this will be clearly stated by the teacher when setting it via Teams.

Assessments and Examinations

During tests, assessments, or formal examinations, device use is permitted only where explicitly authorised in advance by the supervising teacher or examinations team. Any unauthorised use of a device during an assessment may be treated as academic malpractice.

Misuse and Sanctions

Use of a personal device on school premises is a privilege, not a right, and the School reserves the right to withdraw that privilege where the terms of this policy are not observed.

Personal devices are a valued part of learning at The English School, and most students use them responsibly and with purpose. To ensure that this remains the case for everyone, the School has established a clear and proportionate framework to address the occasions where devices are used outside the expectations set out in this policy. This framework exists not to penalise, but to protect the learning environment, support student wellbeing, and reinforce the values of respect and responsibility that underpin life at the School. All members of staff apply it consistently and with fairness, and any incidents are recorded to ensure that responses are informed and appropriate.

The aim in every case is to help students understand the expectations, restore positive behaviour, and ensure that the learning of all is protected.

Level	Trigger / Behaviour	Sanction
Level 1 — Minor	First instance of using a device without permission; device not set to Do Not Disturb; device used outside the classroom environment without authorisation; non-educational application open without authorisation.	Verbal warning given by teacher. Student reminded of policy.
Level 2 — Repeated Minor	Second instance of the same minor breach within a lesson, or repeated minor breaches across lessons, including repeated use of a device outside the classroom environment.	Device confiscated by the teacher for the remainder of the lesson and returned at the end of the lesson. Parent/guardian notified classroom teacher. Incident logged formally as 2 behaviour points for misuse of device.
Level 3 — Moderate	Using a device for social media, gaming, or messaging during lessons; sharing a device without permission; playing audio without authorisation; distracting other students. Not connected to ES Student WiFi (the only approved WiFi).	Device taken to main office by student. Collection at the end of the day. Incident logged by teacher as 2 behaviour points for misuse of device. HEV to follow up for BYOD privileges suspended for one week.
Level 4 — Serious	Recording or photographing staff or students without consent; deliberate disruption of the learning environment; bypassing School filters or using a personal hotspot; repeated Level 3 behaviour; refusal to hand over device if required.	Device taken to main office by student. Collection at the end of the day. Detention issued by teacher. HEV to follow up BYOD privileges suspended for a minimum of four weeks.
Level 5 — Severe	Sharing, distributing, or publishing recordings of staff or students; accessing or distributing inappropriate, offensive, or unlawful content; cyberbullying; academic malpractice during examinations; circumventing network controls with intent; refusal to hand over device if required.	Device taken to main office by student. Permanent withdrawal of BYOD privileges. Safeguarding procedures activated immediately.

Should a device need to be temporarily removed from a student, the device will be placed in a secure, labelled envelope, sealed in the student's presence, and held safely at the School Main office. A confiscation slip will be provided to the student.

Where a student declines to hand over their device, this will be treated as a Level 4 or Level 5 incident and further breach of the School's Behaviour Policy.

Related Policies

This policy should be read alongside the following School policies and documents:

- Digital Wellbeing Framework
- Academic Integrity Policy
- Behaviour Policy
- Use of AI Tools Policy
- ICT Acceptable Use Policy
- Child Safeguarding Policy
- Anti-Bullying Policy
- Data Protection Policy
- Online Safety Policy

Appendix A: Parent and Student Frequently Asked Questions (FAQ)

1. What is BYOD?

BYOD stands for Bring Your Own Device. It allows students to bring their own approved digital device to school to support teaching, learning, collaboration, research, organisation and assessment. The aim of BYOD is to enhance learning opportunities and help students develop the digital skills required for higher education, employment and everyday life.

2. Why has the school introduced BYOD?

Technology is an important component of modern education. BYOD enables students to access learning resources more easily, collaborate with teachers and classmates, develop digital literacy skills, use subject-specific applications, organise notes and coursework efficiently, and access Microsoft 365 tools both in and outside school. BYOD supports learning but does not replace high-quality teaching, discussion, practical activities or traditional learning methods.

3. Which devices are permitted?

The School will publish a list of approved devices and minimum requirements annually. Generally, devices should support current operating systems, be capable of running required educational applications, have a camera and microphone, be protected by a password, PIN or biometric security, and be kept in good working condition. Devices must not be fitted with an eSIM, SIM card, or any other means of independently connecting to external mobile networks.

4. Does my child need a particular brand of device?

No. The school does not require a specific manufacturer. The device simply needs to meet the published technical requirements and be able to access the school's digital learning platforms.

5. How much should families spend on a device?

The school does not prescribe a minimum cost. Families should select a reliable device that meets school requirements and suits their budget. More expensive devices do not necessarily provide educational advantages.

6. Who pays for the device?

The device remains the property and responsibility of the student and their family. The school does not provide, replace or repair personal devices.

7. Is insurance recommended?

Yes. Families are strongly encouraged to ensure that devices are covered for accidental damage, loss, and theft. The school accepts no responsibility for damaged, lost or stolen devices.

8. What happens if a device is lost or damaged at school?

Students should immediately report the incident to a member of staff. While the school will assist where possible, personal devices remain the responsibility of the student and family.

9. Does my child need to bring the device every day?

Yes. Students should bring their device fully charged each day unless instructed otherwise by a teacher. Failure to bring a device may affect a student's ability to participate fully in some learning activities.

10. Are charging facilities available?

Limited power outlets may be available in some areas of the school. Students are expected to arrive with a fully charged device that can last throughout the school day.

11. What software must be installed?

The school will provide guidance on required applications. Typically students will need access to Microsoft 365, Teams, OneNote, Notability and subject-specific applications identified by departments. The school will seek to use free or school-licensed software whenever possible.

12. Where should students save their work?

Students are strongly encouraged to save learning materials in Microsoft OneDrive, Microsoft Teams, and OneNote, and should back up important work regularly. Computer failure is not normally accepted as a reason for missing deadlines.

13. Can students use their device outside the classroom, for example during breaks?

No. Devices are for use within the classroom environment, under the direction of a teacher, only. Devices may not be used in corridors, communal areas, or during breaks. This supports students' wellbeing by encouraging face-to-face socialising and reducing overall screen time during the school day. See the Digital Wellbeing Framework for the reasoning behind this expectation.

14. Can students use social media during school hours?

No. Social media use during lessons is not permitted unless expressly required for an educational activity approved by a teacher.

15. Can students play games on their devices?

Gaming is not permitted during lessons unless it is teacher-directed, educationally purposeful, and part of a supervised learning activity.

16. How much time will students spend using devices in lessons?

Teachers are conscious of the amount of time devices are used in each lesson and make sure that device use is purposeful and balanced with other learning activities. Some subjects or activities, such as Computer Science or project-based lessons, may naturally involve more extended device use. See the Digital Wellbeing Framework for the School’s approach to screen time.

17. Is there a homework-specific channel on Teams?

Yes. Each class team maintains a dedicated Homework channel on Microsoft Teams, used exclusively for setting and submitting assignments, so that homework communication is kept clearly separate from general class updates.

18. Will we know if a homework task requires a lot of screen time?

Yes. Where a homework assignment requires a significant amount of screen time, this will be clearly stated by the teacher when it is set via Teams.

19. Will teachers respond to messages in the evening?

Teachers are not expected to check or respond to student or parent messages after 18:00 on school days. Messages sent after this time will normally be addressed on the next school day.

20. How does the school protect students online?

The school operates a range of safeguards including internet filtering, network monitoring, malware protection, safeguarding systems, and staff supervision. While every effort is made to protect students, no filtering system can provide complete protection. Partnership between school and parents remains essential.

21. Will BYOD increase cyberbullying?

BYOD does not change the school's expectations for behaviour. Cyberbullying is treated as seriously as any other form of bullying and will be addressed in accordance with the school's Behaviour, Safeguarding and Anti-Bullying policies. Students are encouraged to report concerns immediately.

22. Are students allowed to use Artificial Intelligence (AI) tools?

Yes, when permitted by teachers and used appropriately, for example for brainstorming ideas, revision, feedback on drafts, or language support. Students must not submit AI-generated work as their own or use AI in assessments unless specifically authorised. All AI use must comply with the school's Use of AI Tools Policy.

23. Do teachers receive training on using AI tools safely with student data?

Yes. Teachers are trained in the appropriate use of AI platforms in an educational setting, including how to safeguard students' personal data, avoid inputting identifiable student information into external AI tools, and select platforms that meet the School's data protection standards. This training is reviewed and updated as AI platforms and associated risks evolve.

24. What is expected regarding apps and notifications on my child's device?

Parents and guardians are responsible for the applications, software, and social media platforms installed on their child's device. Notifications from these should be disabled during the school day to minimise disruption, and devices must not be fitted with an eSIM, SIM card, or other means of independently connecting to external mobile networks.

25. What happens if a student misuses their device?

Depending on the seriousness of the incident, consequences may include verbal warnings, device confiscation, loss of BYOD privileges, parent meetings, behaviour sanctions, or safeguarding referrals. Serious breaches such as cyberbullying, inappropriate content, examination malpractice or unauthorised recording may result in significant disciplinary action.

26. Can teachers inspect a student's device?

No. Teachers are not permitted to search or inspect a student's personal device themselves. Where there is reasonable concern regarding safeguarding, academic malpractice, cyberbullying, or serious breaches of school policy, the matter is referred to the School's safeguarding team, who will handle the incident and any device access in accordance with the School's safeguarding, behaviour and data protection procedures.

27. Who can parents contact for support?

Parents should contact the student's Form Tutor for general concerns, the student's subject teacher regarding curriculum-related applications, the IT Support Team for connectivity and platform access issues, and the Assistant Head responsible for Digital Learning for BYOD-related matters.

Appendix B: Parent and Student Agreement Form

The English School — Parent and Student Agreement Form: Use of Tablets in School

This agreement outlines the responsibilities and expectations for students and parents or guardians regarding the use of tablets in school. The purpose of using tablets is to support and enhance learning.

Student Responsibilities

By bringing a device to school, the student confirms that they understand and agree to the following:

- Use their device for educational purposes only during class time, as directed by the teacher, and avoid using it for non-educational activities during school hours.
- Use the device only within the classroom environment, and not in corridors, communal areas, or during breaks and lunchtimes.
- Set their device to Do Not Disturb mode for the duration of the school day.
- Take good care of their device and ensure it is stored safely when not in use.
- Keep their device secure and not share passwords or personal information with others.
- Only use their own accounts and not access, modify, or delete another student's work.
- Ensure their device is fully charged at the start of each school day.
- Keep all applications and software up to date and ensure appropriate security settings are enabled.
- Install any subject-specific applications required by their department, as communicated by the relevant teacher.
- Understand that inappropriate use of their device may result in the loss of device privileges and further disciplinary action in accordance with the School's Behaviour Policy.

Parent and Guardian Responsibilities

By allowing their child to bring a device to school, parents and guardians confirm that they understand and agree to the following:

- Ensure their child's device is in good working condition and adequately protected with a case and appropriate security software.
- Ensure the device has no eSIM, SIM card, or other independent means of connecting to external mobile networks.
- Take responsibility for the applications, software, and social media platforms installed on their child's device, and ensure that notifications from these are disabled during the school day.
- Monitor their child's use of the device outside school hours to encourage responsible and purposeful use.
- Understand that the School is not responsible for loss, theft, or damage to their child's device, and that repair or replacement costs are the responsibility of the family.
- Encourage their child to use technology responsibly and for educational purposes.
- Ensure that any subject-specific applications required by the School are installed on the device in a timely manner.
- Support the School in reinforcing the expectations set out in this policy.

School Responsibilities

The School confirms the following commitments to students and families:

- Provide a secure Wi-Fi network for student use during school hours.
- Monitor internet usage and implement appropriate filtering to promote a safe and positive online environment.
- Guide and support students in the effective and purposeful use of their devices for learning.
- Communicate clearly any subject-specific applications that students are required to install, giving reasonable advance notice and indicating where free or lower-cost alternatives exist.
- Provide clear guidelines and expectations for device use in classrooms and across the School.
- Reserve the right to restrict or suspend device use where the terms of this agreement are not honoured.