HAMILTON
International School

BRING YOUR OWN DEVICE (BYOD) POLICY

Vision

Igniting Passion, Purpose and Potential

Mission

Our mission is to develop caring, lifelong learners and global citizens in a culture of excellence through an international, well-balanced education.

Our Core Values



I am Getting Better



Respectful



Resilient



Global Citizen



Communicator



Collaborator



Emotionally Intelligent

Definition of Learning

Learning at Hamilton is the purposeful, personalized process where learners get better in the good struggle zone.

Document Control Table

Status		Public (school website)
Date Approved		May 2026
Latest Review Date		September 2026
To be Reviewed		August 2027
Linked Documents and Policies		E-Safety Policy Behavior Policy Academic Integrity Policy Safeguarding and Child Protection Policy ISP Group Acceptable Use Policy ISP AI Use and Governance Policy
Version	**Date**	**Comments**
2.0	October 2026	Smoothwall no longer installed on personal devices; network filtering applies instead. Windows 11 now required. Extended to all Secondary students. Privacy, AI, equity, and appendix added. Aligned with ISP Group policies.

1. INTRODUCTION AND PURPOSE

A personal laptop gives Secondary students the independence to research, create, collaborate, and manage coursework in ways that prepare them for university and working life. Used well, it helps students take ownership of their learning, access resources anytime and anywhere, and build the digital skills and habits they will need beyond school.

This policy explains how personally owned laptops are used safely and responsibly at The Hamilton International School. It supports the school's E-Safety Policy and reflects the ISP Group Acceptable Use Policy and the ISP Artificial Intelligence (AI) Use and Governance Policy.

2. SCOPE

- The Bring Your Own Device (BYOD) program applies to **all students in Secondary**, who are required to bring a laptop that meets the requirements in Section 4 to school every day.
- Expectations in this policy are applied in an age-appropriate way, with closer teacher supervision of laptop use in the younger Secondary grades.
- This policy applies whenever a BYOD laptop is on school premises, is connected to the school network, is used for school work, or is used to access school systems such as Microsoft 365, wherever the student is.
- Mobile phones, tablets, smartwatches, and other personal devices are not part of the BYOD program. The Hamilton International School is a mobile phone-free environment for students, as set out in the E-Safety Policy.
- Students and visitors may connect personal devices only to the networks designated for them. Staff use of personal devices for work is governed by the ISP Group Acceptable Use Policy, under which school information must not be stored on personal devices without authorization.

3. DEFINITIONS

Term	Meaning in this policy
BYOD laptop	A personally owned laptop, purchased and owned by the student's family, that meets the requirements in Section 4.
School-owned device	Any device purchased, owned, and managed by the school, including devices lent to students or staff.
School network	The school's wired and wireless (Wi-Fi) networks, including the student Wi-Fi.
School systems	Systems accessed through a school account, including Microsoft 365 (Teams, Outlook, OneDrive, and SharePoint) and school learning platforms.
School use	Lessons, enrichment activities, independent study, research, and coursework, as directed by teachers.

4. DEVICE REQUIREMENTS

4.1 The school's digital environment is built on Microsoft Windows and Microsoft 365. To ensure that every laptop works reliably with school systems, printers, and assessment tools, BYOD laptops must meet the following requirements.

Requirement	Minimum	Recommended
Device type	Windows laptop, or Microsoft Surface Pro or Surface Laptop with a keyboard	—
Operating system	Windows 11 (Windows 10 no longer receives security updates from Microsoft)	Latest Windows 11 updates installed
Processor	Intel Core i5 (12th generation or newer) or AMD Ryzen 5 equivalent	Intel Core i7 or AMD Ryzen 7
Memory (RAM)	8 GB	16 GB
Storage	512 GB SSD	512 GB SSD or larger
Screen	12 inches or larger	13 to 15 inches
Battery	At least 6 hours of real-world use	8 hours or more
Wireless	Dual-band Wi-Fi (2.4 GHz and 5 GHz), Wi-Fi 5 (802.11ac)	Wi-Fi 6 or newer
Camera and audio	Built-in webcam and microphone; headphones or earbuds	—
Software	Microsoft 365 apps accessed with the student's school account; an up-to-date web browser; active antivirus (Microsoft Defender is sufficient)	—
Power	Charger with a 3-pin (Type G) plug, brought to school daily	—
Protection	Protective case or sleeve	Hard-shell case; screen protector

4.2 iPads and other tablets (other than the Surface devices listed above), Chromebooks, MacBooks, and mobile phones do not meet the requirements of the BYOD program.

4.3 Families who are unsure whether a device meets these requirements are encouraged to check with the IT team before purchasing.

5. REGISTERING A DEVICE

5.1 Before a laptop is used in school:

(a) the student and a parent or guardian read this policy and the E-Safety Policy, and complete the Student Acceptable Use Agreement online;

(b) the student brings the laptop to the IT team, who connect it to the student Wi-Fi using the student's school credentials; and

(c) the IT team may check that the laptop meets the requirements in Section 4, that Windows is up to date, and that antivirus protection is active.

5.2 No other device configuration is required to connect to the school network. IT configuration on a personal laptop is limited to the Wi-Fi connection and printer setup. The IT team does not install filtering or monitoring software and does not access personal files.

6. SAFE AND ACCEPTABLE USE

When using a BYOD laptop, students must:

(a) **connect only to the student Wi-Fi during the school day**; never use mobile data, a personal hotspot, another student's hotspot, or any external network; never share a hotspot with others; and never use VPNs, proxy services, or any other tool to bypass the school's filtering;

(b) sign in to school systems only with their own school account, keep passwords private, and use multi-factor authentication where enabled;

(c) save school work to OneDrive or Teams so that it is backed up and accessible if the laptop is lost or damaged;

(d) keep Windows, the web browser, and antivirus protection up to date;

(e) use the laptop in lessons only for school use, as directed by the teacher, and close it when asked;

(f) never photograph, record, or livestream another student or member of staff without their permission;

(g) never access, store, or share content that is illegal, offensive, or inappropriate for school, whether online or stored on the laptop;

(h) not install or use games, file-sharing, or hacking tools while in school;

(i) use AI tools only as permitted by their teachers and the Academic Integrity Policy, declare AI use where required, and never upload personal information or images of other people into AI tools; and

(j) follow the Student Acceptable Use Agreement, the E-Safety Policy, and the Behavior Policy at all times.

7. PRIVACY

- The school respects that a BYOD laptop is personal property. No monitoring software is installed on it, and the school does not monitor the content stored on it.

- When a laptop is connected to the school network, the school applies network-level controls only: it filters websites and online services, blocks known VPNs and proxy services, and logs network activity. It does not control the settings or applications on a personal laptop.
- Activity on the school network, such as the websites visited, and activity within school systems, such as Microsoft 365, is logged and may be monitored whatever device is used, as set out in the E-Safety Policy and the ISP Group Acceptable Use Policy.
- Access to network logs is restricted to authorized IT staff. Relevant information is shared securely with the DSL where there is a safeguarding concern, or with authorized leaders where necessary for an investigation, in accordance with ISP policy.
- Where there is a reasonable concern that a laptop holds content that breaches school rules or presents a safeguarding risk, a designated member of the Senior Leadership Team or the Designated Safeguarding Lead (DSL) may ask the student to show the relevant content, normally with a second member of staff present. The laptop may be held securely until it is collected by a parent, and parents are informed. Where content may be illegal, staff will not view or copy it, and the DSL will follow the school's safeguarding procedures, which may include referral to the relevant authorities in Qatar.

8. THE ROLE OF PARENTS

- School filtering protects a laptop only while it is connected to the school network. Once the laptop is on mobile data, a hotspot, or home Wi-Fi, the school's filtering no longer applies.
- We therefore strongly encourage parents to set up parental controls and age-appropriate restrictions on their child's laptop, for example through Microsoft Family Safety, as these stay in place wherever the laptop is used. Parents should also make sure the laptop is kept up to date with security protections enabled.
- No filtering system can block everything. A new website, game, VPN, or proxy service may remain accessible until it is identified. School filtering is an important safeguard, but it works best alongside parental controls, supervision, and regular conversations at home about responsible use.

9. CARE, SECURITY, AND RESPONSIBILITY

- **BYOD laptops are the sole responsibility of the student and their family.** The school accepts no liability for loss, theft, or damage to a personal device or its accessories, whether on school premises, on school transport, or during school activities. Families are strongly advised to arrange suitable insurance.
- Students must:
    - never leave their laptop unattended, and keep it in a locked locker when it is not in use;
    - protect the laptop with a password or PIN and lock the screen when stepping away;
    - never lend their laptop to, or share it with, another student;
    - bring the laptop fully charged every day, together with its charger; and
    - report any loss, theft, or damage to a member of staff immediately.

- If a laptop is lost, damaged, or not working, it should be repaired or replaced promptly. The student should let their homeroom teacher know so that teachers can make arrangements in the meantime.

10. TECHNICAL SUPPORT

- The IT team supports students with connecting to the student Wi-Fi, printing, and accessing their school account and Microsoft 365.
- The IT team does not repair hardware, install personal software, or resolve problems beyond basic school connectivity. For other issues, families should use the manufacturer's support or an authorized service center.

11. ASSESSMENTS AND EXAMINATIONS

Laptops are used in assessments only when authorized by the teacher. For IB and other external examinations, the awarding body's regulations take precedence, and laptops may not be taken into examination rooms unless specifically permitted.

12. EQUITY AND ACCESS

- No student should be disadvantaged because their family has difficulty providing a laptop. Families in this situation are encouraged to contact the Head of Secondary in confidence to discuss the options available.
- Any device lent to a student by the school is a school-owned device. It will have Smoothwall installed and will be managed in line with the E-Safety Policy.

13. BREACHES OF THIS POLICY

- Misuse of a BYOD laptop is managed under the Behavior Policy and may result in the loss of access to the school network. Any safeguarding concern is referred to the DSL, and illegal activity may be reported to the relevant authorities.

APPENDIX A: BYOD STUDENT AND PARENT AGREEMENT

This agreement is completed online as part of the Student Acceptable Use Agreement. A printable copy is provided below for reference.

Student declaration. I have read and understood the BYOD Policy and the E-Safety Policy. I agree to:

- use my laptop for school use as directed by my teachers;
- connect only to the student Wi-Fi in school and never use mobile data, hotspots (my own or anyone else's), VPNs, or other tools to bypass the school's filtering;
- keep my passwords private and my laptop secure, charged, and up to date;
- never record, photograph, or share images of others without their permission;
- use AI tools honestly and only as permitted; and
- tell a member of staff straight away if I see anything online that worries me.

I understand that misuse may result in the loss of network access and action under the Behavior Policy.

Parent or guardian declaration: I understand that internet access is filtered while the laptop is connected to the school network, and that activity within school accounts may be logged and monitored wherever accessed. I understand the school's recommendation to set up appropriate parental controls for use outside school.

Student name: _____

Grade / Homeroom: _____

Student signature: _____ **Date:** _____

Parent/Guardian name: _____

Parent/Guardian signature: _____ **Date:** _____