



Bring Your Own Device (BYOD)

Policy Policy

2025-26

1. Introduction

RAIS supports the educational use of personal devices through our Bring Your Own Device (BYOD) Program, which enhances learning while maintaining network security and digital responsibility. This policy outlines guidelines for students, staff, and parents regarding the appropriate use of personal devices on school premises.

2. Purpose

- ✔ Promote flexible learning opportunities
- ✔ Develop responsible digital citizenship
- ✔ Ensure cybersecurity and data protection
- ✔ Maintain equitable access to technology
- ✔ Support 21st-century skill development

3. Scope

Applies to:

- ◆ Students (Grades 1–12) – Mandatory participation
- ◆ Teachers & Staff – Optional use for instruction
- ◆ Parents/Visitors – Limited guest network access

4. Approved Devices

Device Type	Requirements
Laptops	Windows 10+/macOS 12+, 4GB RAM, 128GB storage
Tablets	iPad (7th gen+), Android 10+ (8" screen min)
Chromebooks	Auto-update enabled, Google Admin support
Phones	Not Allowed

✗ Prohibited Devices:

- Gaming consoles

- Jailbroken/Rooted devices
- Devices with unauthorized software

5. BYOD User Agreement

A. Student Responsibilities

- ✓ Install school-mandated security software
- ✓ Charge devices fully before school
- ✓ Use only RAIS-secured WiFi (no personal hotspots)
- ✓ Follow classroom device protocols (teacher-directed usage)

B. Parent Responsibilities

- ✓ Ensure device meets minimum requirements
- ✓ Monitor home internet use for safety
- ✓ Label devices with student name
- ✓ Provide protective case

C. School Responsibilities

- ✓ Provide technical support for connectivity
- ✓ Offer loaner devices if needed
- ✓ Maintain content filtering on all networks

6. Network & Security Policies

Policy	Details
Network Access	Separate VLANs for students/staff
Data Privacy	No personal data stored on devices
Monitoring	Activity logs retained for 30 days
Updates	Critical patches must be installed within 7 days

7. Classroom Implementation

A. Teacher Guidelines

- Set clear device-use signals (e.g., "45° angle" = attention)
- Use collaboration tools (Nearpod, Kami, OneNote)
- Provide non-digital alternatives when needed

B. Acceptable Use

- ✓ Research & e-books
- ✓ Collaborative projects
- ✓ Assessment platforms

✗ Prohibited Use:

- Social media during class
- Unauthorized recordings
- Cheating/plagiarism

8. Incident Management

Issue	Response
Lost/Stolen Device	Report within 1 hour; school not liable
Cyberbullying	Immediate referral to Social Worker
Hacking Attempts	Device confiscation + disciplinary action
Malware Infection	Quarantine device; IT disinfects

9. Support & Repairs

Tech Help Desk Hours:

📍 Location: IT Office (Bldg. A)

🕒 Times: 7:30 AM–3:30 PM (Sun–Thu)

Note: School does not repair hardware damage.

10. Policy Compliance

All violations will be subject to consequences in accordance with the school's behaviour policy.

Approval and Review	
Review date	May 25 th 2025
To be reviewed on:	May 25 th 2026
Approved as Policy by:	Principal: Mohannad Al Jayousi 