Smart Attendance Device - Orange Pi 5 (User & Developer Manual)

1. How to Burn Code on Orange Pi 5

1. Download and install **Balena Etcher** or **Rufus** on your laptop/PC.
2. Download the **Orange Pi 5 Debian/Ubuntu Image** from the official Orange Pi website.
3. Insert a microSD card (≥32GB, Class 10) or NVMe SSD into your PC.
4. Use Etcher to flash the OS image onto the storage.
5. Insert the flashed storage into the Orange Pi 5.
6. Connect HDMI display, keyboard, and mouse for first boot.
7. Boot and configure: set up **SSH** and **Ethernet LAN** for programming.
8. Transfer your Python/C code via **SCP** or **GitHub**.
9. Use **systemd** to auto-start the attendance software at boot.

2. Peripherals & Installation

Camera (Face Recognition): Connect IMX219/OV5647 to MIPI CSI port, enable drivers in /boot/config.
Fingerprint Sensor: R307 via UART pins or USB. Install Python libraries (pyfingerprint).
NFC/RFID Reader: PN532/RC522 via SPI/I2C. Use 'pi-rc522' or 'pynfc' library.
Ethernet: Plug Cat6 cable into RJ45 LAN port.
Mini LCD Display: Connect via HDMI or SPI (Waveshare drivers).
Buzzer & LEDs: GPIO pins with resistors. Control via RPi.GPIO equivalent (OrangePi.GPIO).
UPS & Battery: Attach UPS HAT with Li-ion 5000mAh battery for backup.

3. Casing & Design

- General Size: ~18cm x 15cm x 10cm (cuboidal).
- Outer Case: Iron or Aluminium-foil coated for **EMI & RFID-proofing**.
- Ports: Only 3 slots (Ethernet, Power, Display).
- Shockproofing: Internal components mounted on standoffs; voids filled with foam/rubber.
- Bigger Outer Safety Box: Device enclosed inside, with additional padding.

4. Features & Benefits

- **Secure Identification:** Face, fingerprint, and NFC multi-factor verification.
- **RFID-proof Case:** Prevents cloning with Flipper Zero & similar devices.
- **No Exposed Ports:** Only functional cables exposed, prevents tampering.
- **Ethernet Only:** More secure than Wi-Fi, prevents remote hacking.
- **Custom NFC:** Only reads unique pre-coded student IDs, rejects fake master keys.
- **Auto Logging:** All attendance securely stored and pushed via LAN.
- **Shockproof Design:** Survives accidental drops & tampering attempts.
- **Judge-Winning Edge:** Combines Security, Reliability, Innovation, Scalability.

5. Why Should Judges Select Our Project?

This project uniquely combines **anti-tamper design**, **secure authentication**, and **scalable deployment**. The case is RFID/EMI proof, with no exposed ports, shock protection, and Ethernet-only connectivity. Judges will value **reliability, child safety, real-world applicability, and technical robustness**. This solution is **tamper-proof, future-ready, and replicable at scale**.