POLICY NAME	ISAWHIS Data Protection Policy
POLICY NUMBER	08.005
SCHOOL	ISAWHIS
TITLE OF STAFF RESPONSIBLE	Head of IT
APPROVING BODY	SLT
EFFECTIVE DATE	6.11.2026
REVIEW DATE	Yearly

ISA Wuhan International School (ISAWH) – Data Protection Policy

1. Scope and Core Principles

This Data Protection Policy applies to all students, staff, administrators, and third parties interacting with ISA Wuhan International School (ISAWH). ISAWH is committed to protecting personal data, maintaining digital privacy, and ensuring the ethical, secure, and transparent handling of all personal and instructional data across school operations.

2. Information Security & Access Controls

- **User Accounts & Authentication:** Access to corporate and academic data requires personalized username and password authentication. Passwords must be at least 8 characters long, contain uppercase and lowercase letters, numbers, and symbols, and must be changed every 180 days. Re-using previous passwords or sharing credentials via email or chat software is strictly prohibited.
- **Network Access & SSIDs:** WiFi access is segregated based on user roles:
    - ISAWH-STAFF: Dedicated wireless network for authorized staff accounts.
    - ISAWH-GUEST: Designated network for guest devices.

- Accounts and network privileges are actively maintained and revoked immediately upon exit.

- **Device Security & Physical Protection:** School-issued laptops, desktops, and mobile devices (e.g., iPads, Macs) must remain under employee or student control or be securely locked in rooms/cupboards when unattended. Computers automatically lock after 5 minutes of inactivity.
- **Centralized Data Storage & Backup:** All staff must save important work files to OneDrive to prevent data loss in the event of hardware failure.

3. Specialized Data Handling Protocols

A. Biometric & Facial Recognition Data

- **Usage & Scope:** Facial recognition technology is strictly limited to Hikvision access control (campus entry/exit) and ManKeBao dining payment systems.
- **Consent & Encryption:** Data collection requires prior written parental/guardian consent. Facial feature data is stored on encrypted, on-campus dedicated servers with strict role-based access restricted to authorized IT and school administration personnel.
- **Audit & Retention:** Usage logs undergo mandatory end-of-semester audits. All biometric facial data is permanently deleted within 30 days of a student's graduation or departure.

B. Student Learning & Management Systems (LMS)

- **Platforms:** Primary academic data, student attendance, assessment records, teacher

comments, and report cards are maintained securely within platforms such as ManageBac.

- **Access Control:** Role-based access ensures that student data is accessible only by authorized educators, coordinators, and administrators.

4. Digital Citizenship, Academic Integrity & AI Ethics

- **Device Loan Agreements:** Students using school-issued devices must sign a Device Loan Agreement committing to the school's Digital Citizenship Code of Conduct.
- **Content Filtering & Safety:** Campus network infrastructure and Managed Devices (via MDM) utilize content filtering to block inappropriate, adult, violent, or unsafe content.
- **Academic Integrity & Citation:** Students are required to present authentic work. Unattributed use of external sources or software constitutes academic dishonesty. ISAWH adheres to MLA referencing conventions across all subjects.
- **Generative AI Policy:** AI tools are permitted as learning aids under a transparent, principled framework ("Think, Generate, Edit"). Students must clearly attribute any AI-generated text, images, or ideas with inline citations and full bibliographic references (specifying the tool, prompt, and date generated).

5. Roles, Incident Reporting, and Review

Stakeholder / Role	Primary Responsibilities
Head of IT / IT Dept.	Manages infrastructure security, access credentials, platform vetting, system backups, and device maintenance.
Staff & Educators	Protect account security, enforce age-appropriate digital safety, and monitor proper student use of IT assets.
Students & Parents	Maintain credential secrecy, follow device agreements, uphold academic integrity, and report suspicious activities or lost hardware immediately.

- **Incident & Vulnerability Reporting:** Any hardware damage, loss, unapproved site discovery, or security concern must be immediately escalated to the IT Department. Unidentified or suspicious email attachments must not be opened and should be forwarded to IT.
- **Policy Review:** This policy is subject to ongoing review and updates to align with technology advancements, local regulatory standards, and IB framework guidelines.