



Safe AI Usage Policy

AI Operations & Data Security

Administrative Staff

Purpose & Administrative Scope

This policy governs the operational and administrative use of Artificial Intelligence across non-teaching departments at Buds Public School, including Admissions, HR, Finance, Facilities, IT, and School Communications.

Data Security Mandatory Standard: Administrative staff handle sensitive institutional, financial, and personal data. Strict adherence to UAE Data Laws is mandatory across all administrative functions.

Data Classification & UAE PDPL Compliance

Under the UAE Personal Data Protection Law (PDPL, Federal Decree-Law No. 45/2021), all data handled by Buds Public School is classified as follows:

Data Classification	Examples	AI Processing Rule
Strictly Confidential	Student PII, medical records, staff salaries, financial accounts.	Absolutely prohibited from public AI models.
Internal Operational	Class schedules, facility maintenance logs, policy drafts.	Permitted only on IT-approved enterprise AI platforms.
Public Information	Published prospectuses, school event calendars, news releases.	Permitted for AI drafting, formatting, and translation.

Permitted vs. Prohibited Operational Use Cases

- Permitted: Using AI to format generic email templates, proofread administrative reports, generate spreadsheet formulas, or translate public notices.
- Prohibited: Uploading un-anonymised student enrolment files, employee performance reviews, financial audits, or confidential KHDA regulatory correspondence into public AI tools.
- Prohibited: Relying on automated AI decision-making for admissions filtering, staff hiring, or financial approvals without human review.

Procurement & IT EdTech Vetting Protocol

No non-teaching staff member may procure, download, or integrate any third-party AI software, browser extension, or cloud service without written approval from the IT Coordinator and/or the designated Data Protection Officer (DPO).



Cybersecurity & AI-Driven Threat Awareness

Staff must remain vigilant against AI-enhanced cybersecurity threats, including deepfake voice impersonation (seeking urgent financial transfers), AI-generated phishing emails, and prompt injection attacks targeting school databases.

Operational Incident Escalation Workflow

Buds Public School - Administrative Data Security Escalation Process

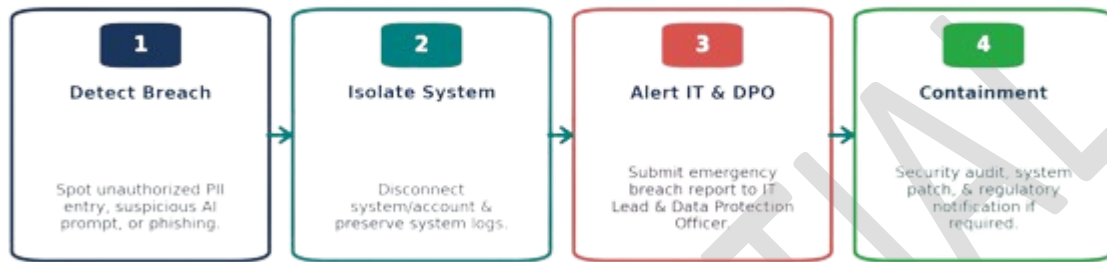


Figure 1: Immediate response protocol for non-teaching staff reporting data breaches or cybersecurity threats.

This policy is grounded in UAE legal frameworks, including the UAE Personal Data Protection Law (PDPL, Federal Decree-Law No. 45/2021), Wadeema's Law (Federal Law No. 3/2016), and KHDA and UNESCO guidelines.

Policy code: BPS/032D/2026

Policy Reviewed: March 2026

Effective from: April 2026

Reviewed By: Senior Leadership Team

Next Review: March 2027

Approved By: Mr. Donald Weilson (Principal)