مدرسة البراعم العامة
Buds Public School

Network Firewall Policy

Scope

Objective: protect students and staff online, ensure age-appropriate access, secure BYOD and school networks, and demonstrate compliance readiness for Dubai private school governance and inspections.

Systems in scope: Sangfor Network Secure v8.0.95 NGFW and Sangfor IAG v13.0.80, Google Workspace, single internet breakout via Etisalat, guest and managed Wi Fi SSIDs, and on-prem devices including CCTV and biometrics.

Governance and compliance

- KHDA linkage: this policy supports student safety, appropriate use, privacy, and school leadership accountability as required for private schools operating in Dubai; inspection ready reports will be maintained.
- UAE school digital practices: control areas mirror identity-based access, content filtering, logging, incident response, change control, and data protection commonly referenced in UAE education digital guidelines.

Network Overview

- Users: 1,200 students, 100 teachers, 15 admin/staff; BYOD permitted for both students and staff with posture enforcement on IAG.
- Topology: single VLAN at present with policy enforced at IAG; SSIDs include guest, staff, management, and four student phase SSIDs (Phase 1–4); inter VLAN design is planned for Phase 2 segmentation.

Role-Based Access Control

- Identity model: IAG authentication with school Google accounts for students and staff; role membership used to assign web and application policies across phases and departments.
- Minimum privilege: staff elevated access is scoped by role; management traffic follows a reduced inspection profile yet maintains threat and malware category controls.

Content Filtering By Phase

- Phase 1 (KG/early years): only child appropriate content allowed; strict categories blocked (adult, gambling, proxy/VPN, malware, command and control, torrents, P2P, gaming), SafeSearch and YouTube strict enforced.
- Phases 2–4: educational access with broader categories as needed; VPN/proxy/torrent/gaming remain blocked; SafeSearch enforced, YouTube strict for students, moderate for staff.

Safesearch And Youtube Enforcement

- Force Google SafeSearch using DNS/header enforcement network wide; YouTube Restricted Mode set to strict for students and moderate for staff to balance teaching needs with safety.

- Enforcement methods may include DNS CNAME to forcesafesearch.google.com and HTTP header injection by IAG where supported.

Application And Circumvention Controls

- Block categories and apps: VPN clients, proxy tools, P2P/torrents, unauthorized remote tools, cryptomining, high risk file sharing; permit remote tools for IT only with explicit app control entries.
- Traffic shaping: throttle social media for staff (reduced bandwidth) while retaining necessary access for communications and outreach.

TLS Inspection Matrix

- Students: HTTPS decryption ON for all phases to allow granular filtering and threat detection.
- Staff: HTTPS decryption ON with defined exemptions; Management: OFF except category/threat checks; Guest: ON to prevent circumvention and ensure accountability.

TLS Inspection Exemptions

- Bypass list: banking, healthcare, e payment gateways, exam/testing platforms that break under decryption, and mandated government portals as needed; these remain subject to URL categorization and threat intel blocking.
- Process: exemptions require ticket approval and are reviewed quarterly to confirm necessity and scope.

DNS and DoH/DoT policy

- Enforcement: force DNS to internal/ISP resolvers from all subnets; block public DoH/DoT resolvers (e.g., Google, Cloudflare, Mozilla) via application signatures and FQDN blocks, and detect DNS tunneling attempts.
- SafeSearch integration: use DNS methods to lock SafeSearch and combine with HTTPS policy to stop DoH-based bypasses.

Egress And Allowlists

- Destination policy: no geo blocking at present; maintain allowlists for CBSE/KHDA/LMS/exam/payment services and device vendors' update/NTP endpoints; mark exam/payment FQDNs for TLS bypass if required.
- Placeholder entries: Oxford LMS, CBSE portals, KHDA portals, Hikvision update servers, ZKTeco services; finalize with exact FQDNs and ports as they are confirmed.

BYOD Posture Enforcement

- Posture gates on IAG: OS up to date, antivirus active, no VPN client detected, block rooted/jailbroken where detectable; non-compliant devices are quarantined/blocked until remediated.
- MAC bypass: reserved strictly for school IoT (CCTV, biometrics, printers) and not permitted for BYOD devices to prevent identity circumvention.

Segmentation Roadmap

- Phase 2: introduce separate VLANs/SSIDs for IoT/CCTV, biometrics, printers, finance, labs, and exam rooms; apply least access inter VLAN firewall rules and deny lateral movement by default.

- Routing control: inter VLAN routing centralized through NGFW with identity aware policies where feasible.

Guest Access And KYC

- Captive portal: self-registration capturing name, email, mobile; no OTP initially; access bandwidth capped at 40 Mbps per guest and sessions time limited (e.g., 8 hours) with auto expiry.
- Accountability: guest logs retained and linked to registration details for investigation and compliance reporting.

Exceptions Workflow

- Educational purpose: exceptions can be fully opened for the teaching duration with ticket record; non educational: auto expire after 1 day; requests received via email and logged.
- Approval: IT led reviews and approves; logs of exceptions are retained for audit/inspection and quarterly policy review.

Data Protection And Google Workspace Controls

- Data location: Google Drive as primary repository; enable Google Workspace DLP to detect national identifiers (e.g., Emirates ID/passport) and restrict external sharing by default, especially for students and early phases.
- Retention: enable Google Vault/retention where available; export and snapshot critical shared drives periodically to reduce accidental deletion risk.

Logging, Retention, And Alerting

- Retention: minimum 6 months on IAG as currently configured, with a roadmap to 12–24 months via syslog/SIEM export for KHDA audit readiness; prioritize admin/audit and web activity logs.
- Alerts: enable threshold-based alerts for malware detections, DLP violations, brute force anomalies, large data exfiltration, and repeated policy evasion attempts.

Incident Response

- Ownership: IT leads initial triage and response; high severity issues escalate to the Principal within one hour; safeguarding or serious data concerns are reported same day per school governance obligations.
- Playbooks: maintain runbooks for malware outbreak, account compromise, data leak, and online safety incidents; preserve evidence and logs for internal review and inspection requests.

Change Control

- Cadence: NGFW updates every 45 days; IAG every 30 days; rule changes proceed via ticket, risk review, after hours change window, and tested rollback plan.
- Backups: weekly offsite configuration backups; verify restore quarterly to ensure disaster recovery readiness.

Staff Access Policy

- Allowed with shaping: social media and cloud storage for staff, rate limited to protect learning bandwidth; developer and documentation sites permitted for curriculum needs.

- Blocked: adult/illegal content, crypto mining, high risk file sharing; remote tools permitted only for IT by policy signature and denied for other roles.

Student Email And Collaboration

- External email: restricted for students; Drive external sharing blocked by default; Google Meet access aligned to phase (stricter in Phase 1–2, enabled with controls in Phase 3–4).
- Monitoring: audit sharing events and Meet usage for safeguarding triggers in coordination with the safeguarding lead.

Special Systems

- Current state: CCTV (Hikvision), ZKT biometrics, printers, labs, and 3D lab equipment operate on existing VLAN with identity controls at IAG; MAC authentication used for IoT only.
- Roadmap: migrate these to dedicated VLANs with restricted egress; allow only required update/NTP FQDNs and management channels in Phase 2.

Reporting And Reviews

- Reviews: quarterly review of web filter categories, exceptions, TLS bypass lists, and posture policy; produce termly online safety and usage reports for leadership.
- Parent communications: include acceptable use and online safety summaries in admissions/parent handbooks; make filtering and privacy statements available upon request.

Policy code: BPS/012/2025

Policy Reviewed: March 2025

Effective from: April 2025

Reviewed By: Senior Leadership Team

Next Review: March 2026

Approved By: Mr. Donald Weilson (Principal)