AI Use Policy for Administration & Office Staff

King David Schools

1. Purpose & Scope

Why: Administrative and office staff handle sensitive information daily (finance, HR, admissions, learner records, marketing). While AI tools can significantly improve efficiency, they must be used responsibly to avoid breaches of privacy, reputational damage, or misinformation.

How: This policy sets out clear guidelines for using AI securely and ethically in daily operations.

What: Applies to all administration and office staff across HR, finance, admissions, marketing, IT, and other support functions.

Alignment:

- UNESCO 2023: Human-centred and ethical AI (3.1).
- South African POPIA: Protection of personal information.
- OECD & EU AI Act: Risk-based, transparent, and accountable AI usage.

2. Principles

Confidentiality First

- POPIA requires personal and financial data to be protected at all times.
- No restricted or confidential data may be uploaded into public AI tools (e.g., free ChatGPT, Gemini, Claude).
- Only enterprise-approved AI (e.g., Microsoft 365 Copilot with enterprise safeguards) may be used.

Efficiency with Oversight

- AI may assist with drafting, summarising, or scheduling tasks.
- Staff remain responsible for fact-checking, editing, and approving all outputs.
- AI is a support tool, not a decision-maker.

Transparency

- Staff must be able to explain how AI was used in any official output.
- Example: “AI drafted the first version of this newsletter, which I then revised.”

Compliance

- All AI use must comply with POPIA, intellectual property law, and copyright rules.
- International best practice emphasises respecting consent and avoiding misuse of third-party content.

3. **Data Classification & Protection**

- Restricted Data (never used in AI): IDs, medical records, payroll, bank accounts, disciplinary records.
- Confidential Data (only via approved enterprise AI): budgets, draft policies, internal memos, strategy notes.
- Public Data (safe for AI use): published newsletters, website content, or public reports.

UNESCO Link: Institutional responsibilities (3.3).

4. Permitted Uses of AI and limitations

- Communication: Drafting parent notices, newsletters, or social media captions *(staff must finalise wording).*
- Meeting Support: AI notetakers/transcribers in staff meetings *(with prior consent, see list of approved tools).*
- Scheduling: Assisting with timetables or automated calendar invites *(see list of approved tools).*
- Translation: Producing first drafts of multilingual parent communication.
- Finance & Reports: Generating draft templates for budgets, procurement, or survey summaries *(not final decisions, follow data classification rules).*

UNESCO Link: Institutional strategies (5.1).

5. Prohibited Uses of AI

- Uploading confidential data (e.g., salary slips, learner addresses) into unsecured AI systems.
- Using AI to make final HR or financial decisions.
- Generating medical, legal, or disciplinary advice via AI.
- Producing misleading, fabricated, or plagiarised content.

UNESCO Link: Content without consent (2.3).

6. Records Management

- AI-generated work must be exported into official storage systems (SharePoint, Teams, Finance DB).
- Chat histories in AI tools are not official records.
- Final responsibility for archiving remains with staff.

UNESCO Link: Build evidence base (4.7).

7. Accuracy, Bias & Accessibility

- All AI outputs must be fact-checked.
- Language must be reviewed for neutrality, inclusivity, and accessibility (e.g., plain English, no jargon).
- Avoid stereotypes, racist or derogatory or biased phrasing from AI-generated drafts.

UNESCO Link: Promote plural opinions (4.6).

8. Incident Response

- If staff suspect a data breach (e.g., confidential file uploaded to a public AI):
  - Immediately notify the IT Department and Data Protection Lead.
  - Complete a Data Breach Report (aligned with POPIA requirements).
- Non-disclosure of a breach may be treated as misconduct.

UNESCO Link: Institutional user responsibilities (3.3.3).

9. Training & Support

- Annual training for all staff on:
  - Safe AI use.
  - Data protection (POPIA refresher).
  - Ethical and inclusive communication.
- Regular workshops on new AI features.

UNESCO Link: Build capacity for staff (4.5).

10. Monitoring & Audit

- AI use will be audited twice a year by IT and EdTech.
- Random spot-checks on outputs may be conducted to ensure compliance.
- Policy reviewed annually to align with new laws and technologies.

UNESCO Link: Long-term implications (4.8).

11. Communication & Consent

- Parents, staff, or external stakeholders must be informed if AI notetakers or transcription tools are used in meetings.
- Consent is required before recording or transcribing.

UNESCO Link: Individual user consent (3.3.4).

12. Consequences of Misuse

- Accidental misuse (e.g., using unapproved AI for non-sensitive drafts): retraining provided.
- Serious breaches (e.g., uploading salary records to ChatGPT): treated as a POPIA violation and may result in disciplinary action.
- Persistent misuse: could result in suspension or termination, as has occurred in international cases (Samsung, 2023, engineers uploaded confidential code into ChatGPT).