RIFUMO
EMPOWERMENT HOLDINGS (PTY) Ltd

BID NUMBER: GT/GDEG/016/2026

BID DESCRIPTION: THE ENHANCEMENT, SUPPORT AND MAINTENANCE OF THE GDE ONLINE ADMISSION SYSTEM VIA THE MICROSOFT ENTERPRISE AGREEMENT FOR A PERIOD OF 36 MONTHS

TERM: 36 MONTHS

CLOSING DATE & TIME: 21 APRIL 2026, 12:00 PM

Table of Contents

1 Rifumo Empowerment Holdings

Established in 2013, Rifumo Empowerment Holdings (REH) is an Information Technology firm specializing in Process Automation (PA), Business Intelligence (BI), eCommerce Solutions, Data Warehousing (DW), Digitization, Customer Relationship Management systems (CRM), Application Development and Microsoft Business Central (BC). Our expertise in the development and implementation of Microsoft Technology (MT) enables our team to utilize standard best practices in the implementation of new technology and innovation. REH is a 100% black-owned SMME, B-BBEE Level 1 contributor and a Microsoft Gold Partner.

REH excels in development, customization, configuration, and implementation of technology solutions that offer expert guidance on the latest developments in technology across multiple industries. The organization provides tailor-made solutions that are user-centric and customer focused, to enable digital transformation using standard best practices and tried and tested methodologies.

We provide innovative technology through dedicated partnerships with our clients as we work to achieve outcomes that are user-driven and cost-effective. We take pride in enabling solutions and sharing knowledge collaboratively with our clients.

1.1.1 Proven Track Record

Rifumo has a proven track record and strong credentials in Microsoft Dynamics 365 projects, eCommerce, ICT Assessments, Business Process Design, System Integrations, and Project Management techniques. We remain a partner of choice to several Public Sector Clients. Our clientele base includes but is not limited to the following.

- Johannesburg Development Agency JDA
- City of Johannesburg Departments
- Public Investment Corporation
- Gauteng Department of Education

1.1.2 Our Solid and Robust Methodology

Our Project Management and Implementation methodology is based on the Microsoft Operations Framework and the Dynamics Sure-Step toolsets. These are tried, tested, and trusted methodologies which have, over the years been utilized, and proven to add the desired value to Clients.

1.1.3 Our Services Catalogue

Microsoft Azure Cloud Services:

We provide comprehensive implementation and support for Microsoft Azure's suite of cloud services, including virtual machines, storage, databases, analytics, AI, IoT, and more. We enable organisations to build, deploy, and manage applications and infrastructure in a secure and scalable cloud environment.

Microsoft 365:

We offer Office 365 implementation services, to combine productivity tools such as Word, Excel, PowerPoint, and Outlook with collaboration services like SharePoint, Teams, and OneDrive. This is done in collaboration with our partners (clients) to enable businesses with cloud-based communication, collaboration, and productivity solutions.

Dynamics 365:

We offer an end-to-end Dynamics 365 (CRM and ERP) suite of intelligent business applications that streamline processes and enhance customer relationships. This includes modules for sales, marketing, customer service, finance, supply chain, and more, enabling organizations to optimize their operations and drive growth.

Business Intelligence:

We offer technologies, applications, and practices that enable organisations to collect, analyse, and interpret data to make informed business decisions. This involves the use of various tools (Microsoft BI tools) and techniques to transform raw data into meaningful insights, helping businesses gain a competitive edge and drive growth.

Azure AI and Machine Learning (AI and ML):

Through the use of Microsoft Azure (AI and ML), we provide a robust set of AI and machine learning services, including Azure Cognitive Services and Azure Machine Learning. These services enable developers to build intelligent applications that can understand, reason, and interact with users in a natural and personalized way.

Azure IoT:

We use Azure IoT to provide a comprehensive set of services and tools for building and managing IoT solutions. This enables our BI and technical team help organisations to connect, monitor, and manage devices, collect, and analyse data, and create actionable insights to drive operational efficiency and innovation.

Power Platforms:

We use Microsoft Power Platform to combine Power Apps, Power BI, and Power Automate (formerly known as Microsoft Flow) to create low-code/no-code solutions for building business applications, data visualizations, and workflow automation. This empowers organisations and users to create custom solutions and drive digital transformation without extensive coding skills.

Microsoft Security Services:

We provide a range of security services and solutions to protect against evolving threats. This includes Azure Security Center, Microsoft Defender for Endpoint, Microsoft 365 Defender, and more, helping organisations safeguard their data, identities, and infrastructure. This is done through innovation and partnerships with other leading technology organisations in the cybersecurity sector.

Data Warehousing:

We offer data warehousing services for the collection, to collecting, organising, and storing of large volumes of structured and sometimes unstructured data from various sources within an organisation. This involves creating a central repository, as a data warehouse, which is designed to support business intelligence, business portals, analytics, and reporting.

TABLE 1: COMPANY PROFILE: OUR SERVICE CATALOGUE

1.1.4 Business Professional Services

We are a premier provider of comprehensive business services, dedicated to enhancing organizational efficiency and effectiveness.

Our core offerings include:

- **Project Management Office (PMO)**: Establishing and maintaining a centralized PMO to ensure consistent project delivery, alignment with strategic goals, and optimal resource utilization.
- **Vendor Management**: Developing and managing vendor relationships to ensure quality, compliance, and cost-effectiveness, while mitigating risks associated with third-party engagements.
- **Governance**: Implementing robust governance frameworks to ensure accountability, transparency, and adherence to regulatory requirements across all business operations.
- **Budget Management**: Providing expert financial oversight, including budgeting, forecasting, and financial reporting, to ensure fiscal responsibility and support strategic decision-making.

we pride ourselves on our ability to deliver tailored solutions that meet the unique needs of our clients. Our team of experienced professionals is committed to driving excellence and fostering sustainable growth. By partnering with us, businesses can navigate the complexities of today's market with confidence and agility.

1.1.5 Consulting Services

Our consulting services aim to provide organisations and government departments with technological solutions to penetrate and/or improve the delivery of business and government services through the use of technology, with expert guidance on service delivery and business model improvement.

Here is a comprehensive catalogue of service offerings that covers various domains, including:

- Project Management
- Change and Adoption
- Business Intelligence
- eCommerce Solutions
- Enterprise Content Management
- OpenText
- Machine Learning
- Artificial Intelligence
- IoT
- Data Centre Support
- Hosting Solutions
- Modern Workspace (Microsoft 365)
- ICT Infrastructure
- Enterprise Infrastructure Architecture
- Communication Infrastructure
- Disaster Recovery
- Cybersecurity, and
- Healthcare

FIGURE 1: COMPANY PROFILE: CONSULTING SERVICES

These services are designed to cater to the specific needs of organizations across various industries, providing comprehensive solutions and support in their respective domains.

1.1.6 Our Track Record

Below are projects that Rifumo have been involved in, that illustrate our capability and experience in delivering Microsoft solutions.

FIGURE 2: COMPANY PROFILE: OUR FOOTPRINT

1.1.7 Our Business Partners

MTN	Microsoft	Huawei
First Technology	Phakamo Tech	Teraco
Reblaze	OpenText	Archibus
Interfile	Trifour	K2
Nintex	Dynamics Africa	

TABLE 2: COMPANY PROFILE: OUR BUSINESS PARTNERS

2 Executive Summary and Key Introduction

2.1 Introduction

The Gauteng Department of Education (GDE) operates the Gauteng Online Admissions System as a critical citizen-facing platform that enables parents and guardians to apply for learner placement at public schools. The system supports equitable access to education services and must operate reliably during peak admissions periods, where public confidence, policy compliance, and service continuity are essential

The Gauteng Department of e-Government (e-Gov) has invited proposals from suitably qualified service providers for the **enhancement, support, maintenance, and operational sustainability** of the **existing** GDE Online Admissions System for a fixed term of **36 months**, to be procured and transacted via the **Microsoft Azure Marketplace** under the existing **Microsoft Enterprise Agreement (EA**

This proposal is submitted in response to **Bid GT/GDeG/016/2026** and is structured to meet the tender's functionality and demonstration requirements by providing a clear delivery approach, governance model, controlled engineering practices, and a milestone-driven 36-month project plan. It demonstrates how the bidder will implement the required enhancements and modules while ensuring the platform remains **secure, scalable, auditable, and highly available**, with full compliance to public sector governance obligations and data protection requirements

2.2 Executive Summary

2.2.1 Purpose of the Tender Response

The purpose of this procurement is to appoint a technology partner capable of delivering a secure, scalable, auditable, high-availability Online Admissions platform—covering enhancements, operational support, and skills transfer—while complying with public sector governance obligations and the Microsoft Azure Marketplace procurement model.

2.2.2 Our Understanding of the Requirement (Scope and Outcomes)

GDE requires a delivery partner to:

- **Enhance and optimise the existing Online Admissions System**, including identifying and resolving functional bottlenecks and technical challenges
- **Design, develop, deploy, and support new admissions modules**, including:
    - **Grade R applications module** (currently manual)
    - **Inner-grade admissions module** (Grades 2–7 and 9–11
    - **Public Special Schools admissions and placement module**, including referrals and support plans
    - Support for **learner transfers between schools**, where required
- Provide **application-level support, maintenance, and performance optimisation**, including proactive monitoring and responsive support during peak admissions windows
- Ensure the platform meets key baseline capabilities including: web/mobile responsive interfaces, secure registration/authentication, role-based access control, automated SMS/email notifications, comprehensive audit logging, real-time dashboards/analytics, and high concurrency support (60,000+ concurrent users).

2.2.3 Procurement and Commercial Model (Azure Marketplace / EA)

This tender operates under the **Microsoft Azure Marketplace Agency Model**, where Microsoft is responsible for billing, invoicing, tax handling, subscription management, and Azure platform support, while the appointed partner is responsible for solution pricing within Marketplace, technical configuration/implementation, and application-level support and SLA compliance. All mandatory costs must be transacted via Azure Marketplace, and no direct invoicing to GDE is permitted outside the Marketplace model

2.2.4 Delivery Approach Our delivery approach is structured around:

1. **Governed mobilisation and planning**: contract kick-off, governance structures, risk register, milestone acceptance criteria, and an admissions-calendar aligned delivery schedule
2. **Requirements validation and detailed design**: validation of existing platform requirements and confirmation of enhancements/modules, with controlled BRS/FRS/TDS artefacts governed through formal change control.

3. **Controlled engineering practices**: iterative delivery with secure development practices, strict configuration-driven approaches (no hardcoding), version control, release management with rollback procedures, and full traceability between requirements, changes, testing, and deployment evidence.
4. **Testing and operational readiness**: complete functional testing, regression testing, stress/performance testing, and UAT for all enhancements and modules, with defects resolved prior to production deployment and test artefacts retained for auditability.
5. **Go-live and stabilisation support**: controlled system opening and hypercare/stabilisation support during admissions go-live windows
6. **Sustained support and continuous enhancement**: SLA-based L2/L3 support, scheduled maintenance, performance and health reporting, and preventative maintenance throughout the 36-month term
7. **Skills transfer and handover**: mandatory, measurable skills transfer executed from inception to close-out, including documentation, SOPs, training manuals, and formal handover with sign-off.

   Important bidder positioning : While the system is not being replaced or re-platformed, our proposed delivery model will strengthen maintainability and scalability through disciplined modular delivery and event-driven integration patterns *as a delivery approach*, while keeping all work within the existing GDE-owned Azure environment and governance controls.

2.2.5 Key Deliverables

Key deliverables will include:

- **Business Requirements Specifications (BRS)**, **Functional Requirements Specifications (FRS)**, and **Technical Design Specifications (TDS)** as controlled artefacts.
- Enhanced system modules and newly implemented admissions modules (Grade R, Inner-Grade, Public Special Schools).
- Testing artefacts and results (functional, regression, performance, UAT), defect logs, and readiness sign-off packs.
- User and technical documentation, SOPs, training materials, and skills transfer execution records.

- Formal handover and close-out report, including source/configuration artefacts as applicable and signed handover checklist.

2.2.6 Project Duration, Milestones, and Resourcing (36 Months)

The project is delivered over **36 months** with milestone-based delivery aligned to the specification's milestone structure (Year 1 mobilisation/design/enhancement/testing/go-live; Year 2 and Year 3 enhancement cycles with testing/UAT/go-live; and continuous support/maintenance with skills transfer and formal handover).

Resourcing and effort are structured according to the submitted delivery phases and estimated man-days, including:

- Phase 1 (Initiation & Design), Phase 2 (Build & Modules), Phase 3 (Testing/UAT/Go-Live/Stabilisation), and Phase 4 (Support & Maintenance across 36 months).

2.2.7 Pricing Summary (High-Level)

The commercial response is structured as a fully itemised, VAT-inclusive pricing schedule covering:

- Once-off implementation & enhancements,
- Licensing (36 months),
- Hosting & infrastructure (36 months),
- Support & maintenance (36 months),
- Skills transfer & training, with a total mandatory contract value for the full 36-month term as per the submitted pricing schedule.

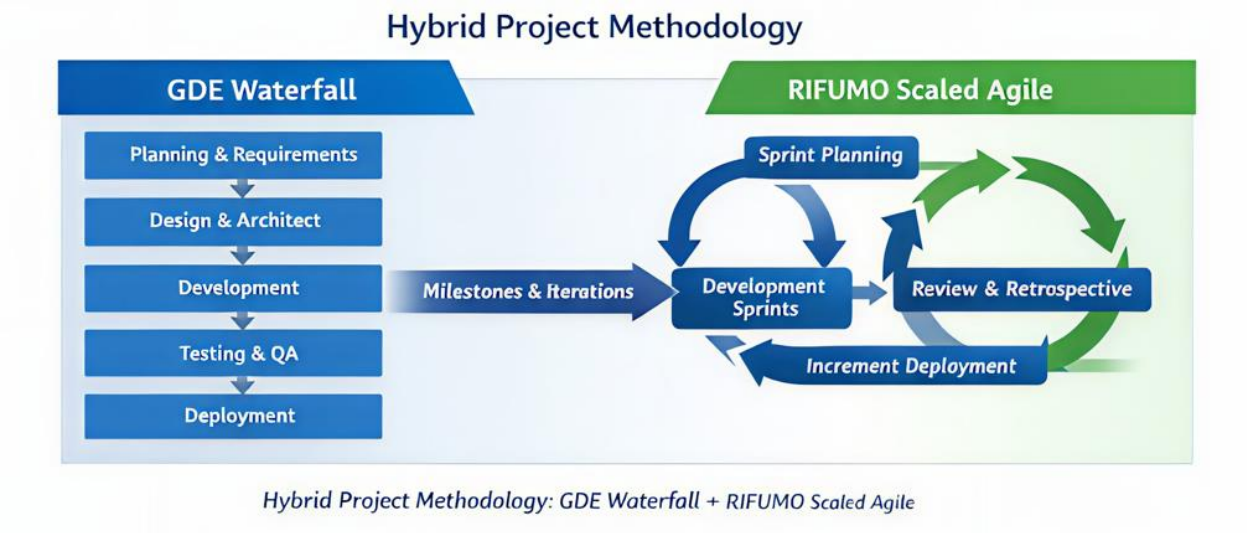
2.2.8 Submission and Compliance Note

The bid pack requires Section 1 and Section 2 to be submitted separately and the proposal submission is required by the stated closing date/time and submission instruction to the SCM contact email address.

3 Approach

3.1 Approach Overview (What we will do and why this works)

Rifumo's approach is designed to meet two equally important requirements in this TOR: **(1) strict governance, traceability, and auditability**, and **(2) the ability to deliver enhancements iteratively and safely across annual admissions cycles over 36 months**. To achieve this, we will apply a **hybrid delivery approach** that combines **GDE-style waterfall stage gates** (formal baselines, approvals, and milestone acceptance) with **scaled agile execution** (timeboxed sprints, incremental releases, and continuous stakeholder feedback



Hybrid Project Methodology: GDE Waterfall + RIFUMO Scaled Agile

This approach ensures we:

- Maintain **controlled project artefacts** (BRS/FRS/TDS, test evidence, documentation) as required deliverables
- Deliver enhancements aligned to the admissions calendar with frequent validation and reduced risk.
- Provide verifiable evidence for **testing, audit logs, and change control**, all of which are explicit expectations in the TOR.

3.2 Governance & Control Model

We will implement **formal stage gates** that ensure governance, approvals, and audit-ready traceability. These gates act as "control points" before moving into build and release.

Stage Gate 1: Mobilisation & Inception

- Establish governance structures, reporting cadence, and project controls.
- Produce and baseline the integrated project plan and milestone acceptance criteria (required for milestone-based invoicing and acceptance).

Stage Gate 2: Requirements Validation & Baseline

- Validate existing platform requirements and confirm Year 1 scope (Grade R, Grade 1/8 enhancements and other agreed enhancements).
- Produce controlled requirements artefacts (BRS/FRS as required by the TOR deliverables).

Stage Gate 3: Design Baseline (Technical & Security Design)

- Produce Technical Design Specifications (TDS) and baselined design decisions, including security, RBAC, audit controls, integration approach, and testing approach.

Stage Gate 4: Release/Go-Live Acceptance

- Move to production only once functional testing, regression testing, performance/stress testing and UAT are completed and accepted, with evidence retained for governance/audit

These stage gates directly align with the TOR's requirement for an iterative yet controlled methodology, governed by approved requirements and change control

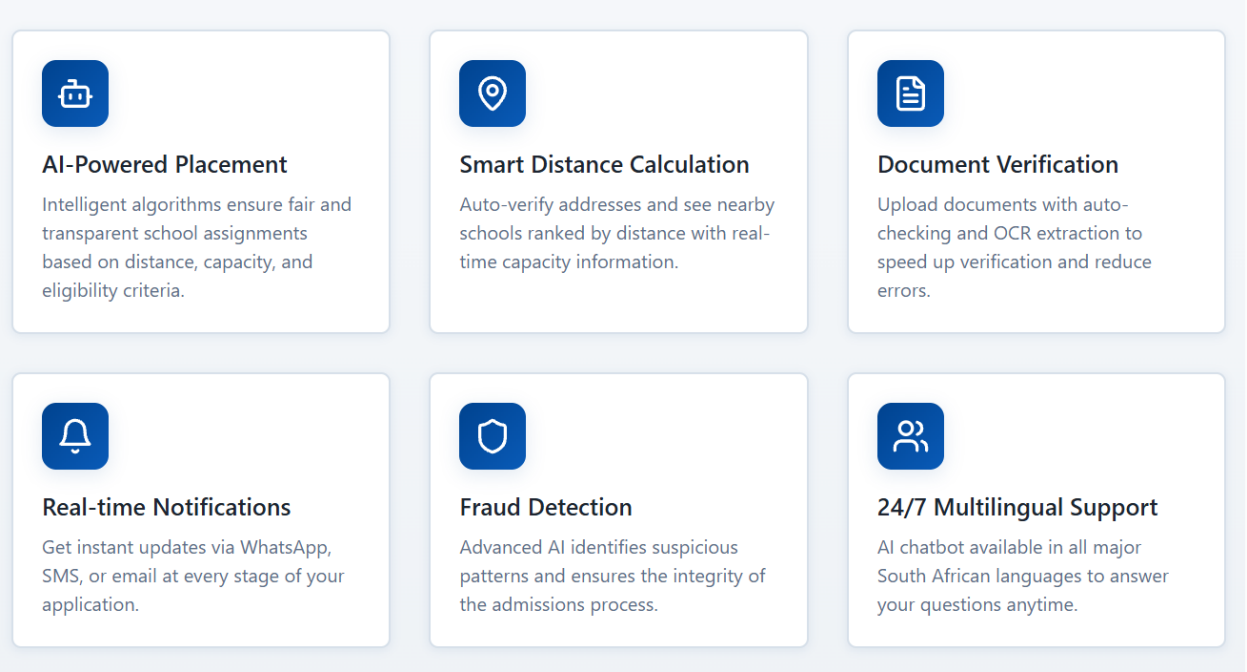
3.3 Scaled Agile Execution

Between the stage gates, delivery will be executed using **scaled agile sprints** (e.g., 2-week cycles) to ensure continuous progress and early validation.

Each sprint will follow a consistent pattern:

1. **Sprint Planning & Refinement:** confirm sprint backlog aligned to approved requirements/change requests
2. **Build & Configuration:** implement enhancements using configuration-driven techniques (no hardcoding) and version control.
3. **Testing within Sprint:** unit tests + developer validation, followed by SIT/regression readiness.
4. **Sprint Demo & Review:** demonstrate delivered increments to stakeholders for early feedback
5. **Incremental Release (Controlled):** release only through approved release windows and controlled processes with rollback procedures. This ensures consistent delivery while protecting system stability during critical admissions periods.

3.4 Features



3.4.1 AI-Powered Placement

Intelligent algorithms ensure fair and transparent school assignments by analyzing multiple factors such as distance from the applicant's home, available school capacity, and eligibility criteria. This system eliminates bias, promotes equity, and guarantees that every child has access to the most suitable school placement.

3.4.2 Smart Distance Calculation

The portal automatically verifies residential addresses and calculates proximity to nearby schools. Parents and guardians can view a ranked list of schools based on distance, along with real-time capacity information. This feature simplifies decision-making and ensures families have accurate, up-to-date data when applying.

3.4.3 Document Verification

Applicants can upload required documents directly to the portal. Advanced OCR (Optical Character Recognition) technology extracts and validates information instantly, reducing manual errors and speeding up the verification process. This ensures compliance with admission requirements while minimizing administrative workload.

3.4.4 Real-time Notifications

Families receive instant updates at every stage of the application process via WhatsApp, SMS, or email. Whether it's confirmation of submission, document approval, or final placement results, applicants stay informed without needing to constantly check the portal.

3.4.5 Fraud Detection

The system uses advanced AI to identify suspicious application patterns, duplicate entries, or falsified documents. This proactive fraud detection protects the integrity of the admissions process, ensuring that placements are awarded fairly and securely.

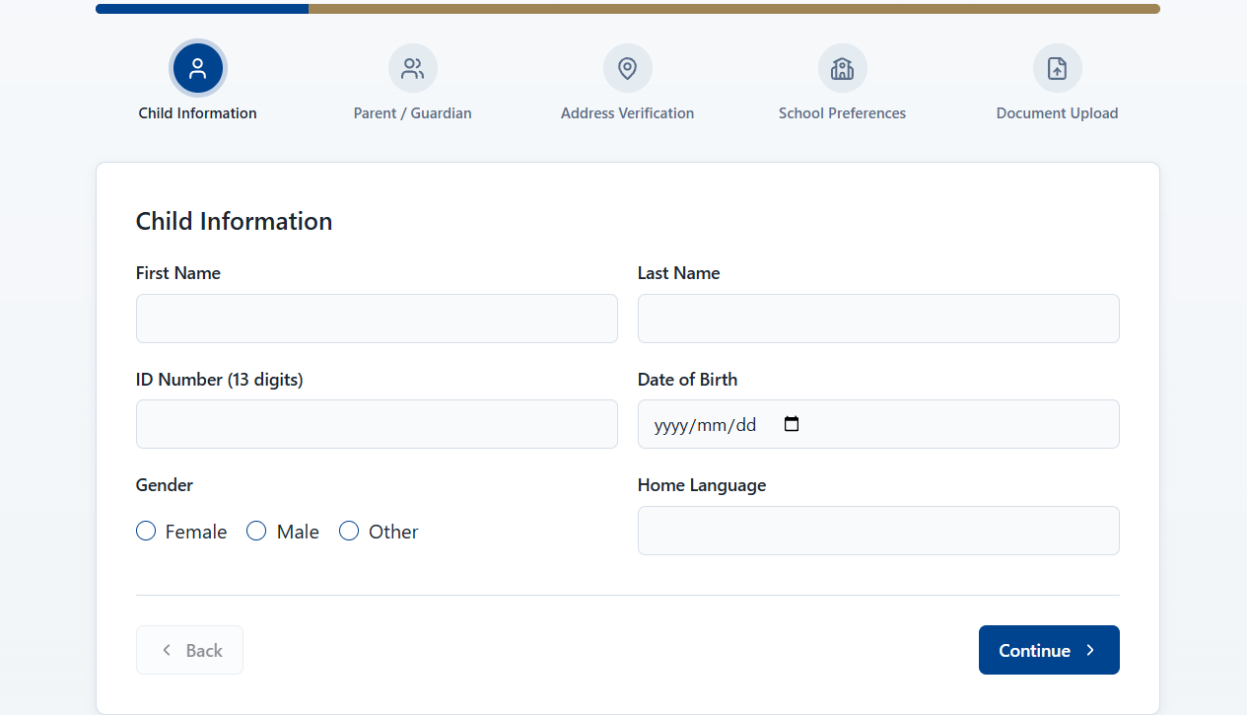
3.4.6 24/7 Multilingual Support

An AI-powered chatbot is available around the clock to answer questions in all major South African languages. Parents and guardians can access guidance anytime, breaking down language barriers and ensuring inclusivity for diverse communities.

3.4.7 Impact

Together, these features create a **transparent, efficient, and user-friendly admissions process** that reduces administrative burden, empowers families with accurate information, and ensures fairness in school placements.

3.5 Application and Tracking

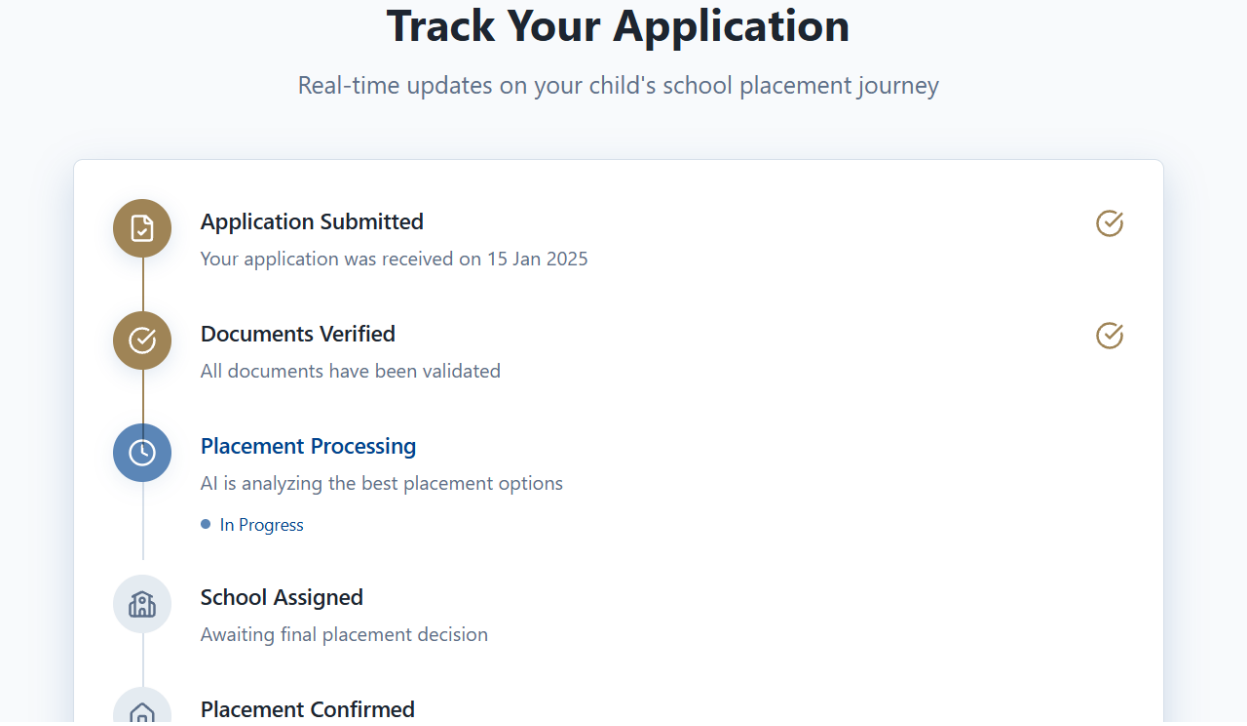


3.5.1 Unified Application Submission

Parents and guardians can complete a single, streamlined application form that automatically distributes information to all relevant schools. This reduces duplication, ensures consistency, and saves time for families and administrators.

3.5.2 Step-by-Step Progress Tracking

The portal provides a clear visual timeline of the admissions journey — from submission, document verification, eligibility checks, placement consideration, to final decision. Each stage is updated in real time, allowing applicants to know exactly where they stand.



3.5.3 Personalized Dashboard

Every applicant has access to a secure dashboard showing their application status, pending actions, uploaded documents, and communication history. This central hub eliminates confusion and ensures families never miss a requirement or deadline.

3.5.4 Multi-Channel Updates

Applicants receive notifications via WhatsApp, SMS, and email whenever their application status changes. This ensures no family is left uninformed, regardless of their preferred communication method.

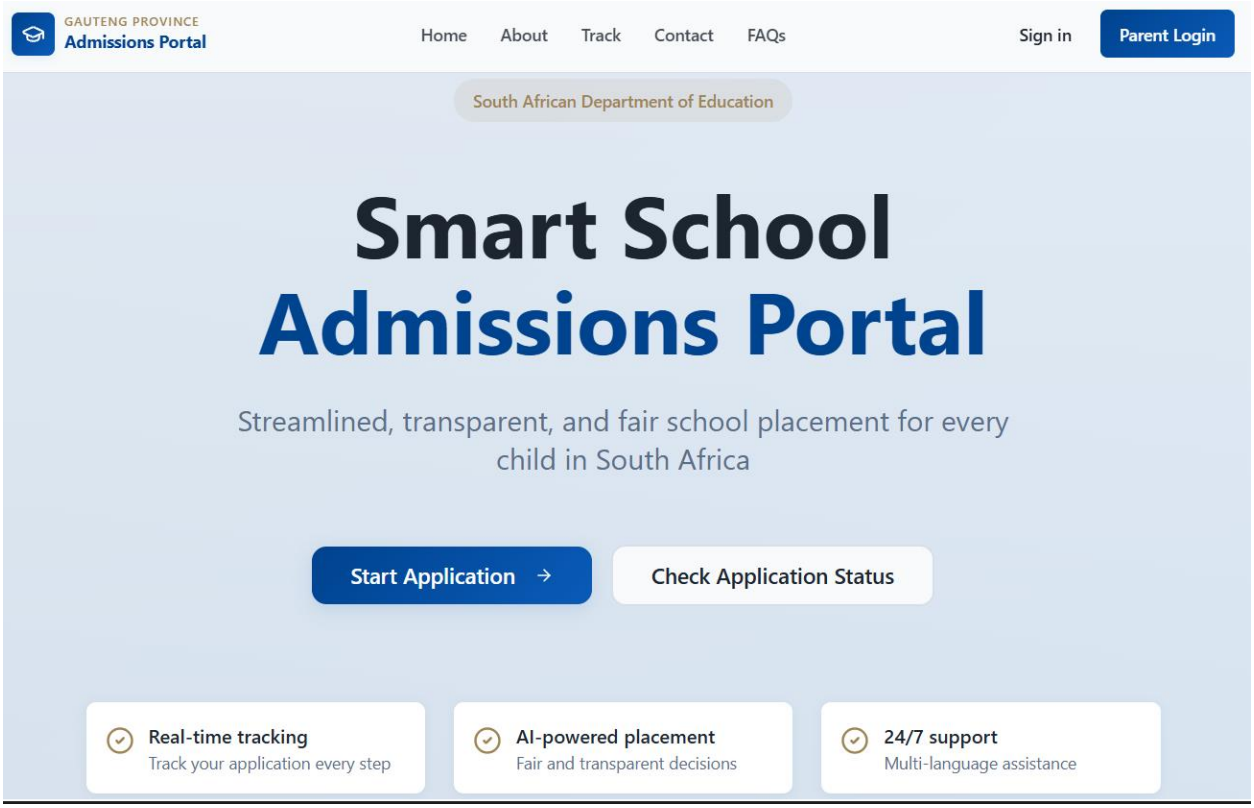
3.5.5 Secure Tracking ID

Each application is assigned a unique tracking ID, allowing parents to quickly reference their case when contacting support or checking progress. This adds transparency and simplifies communication with administrators.

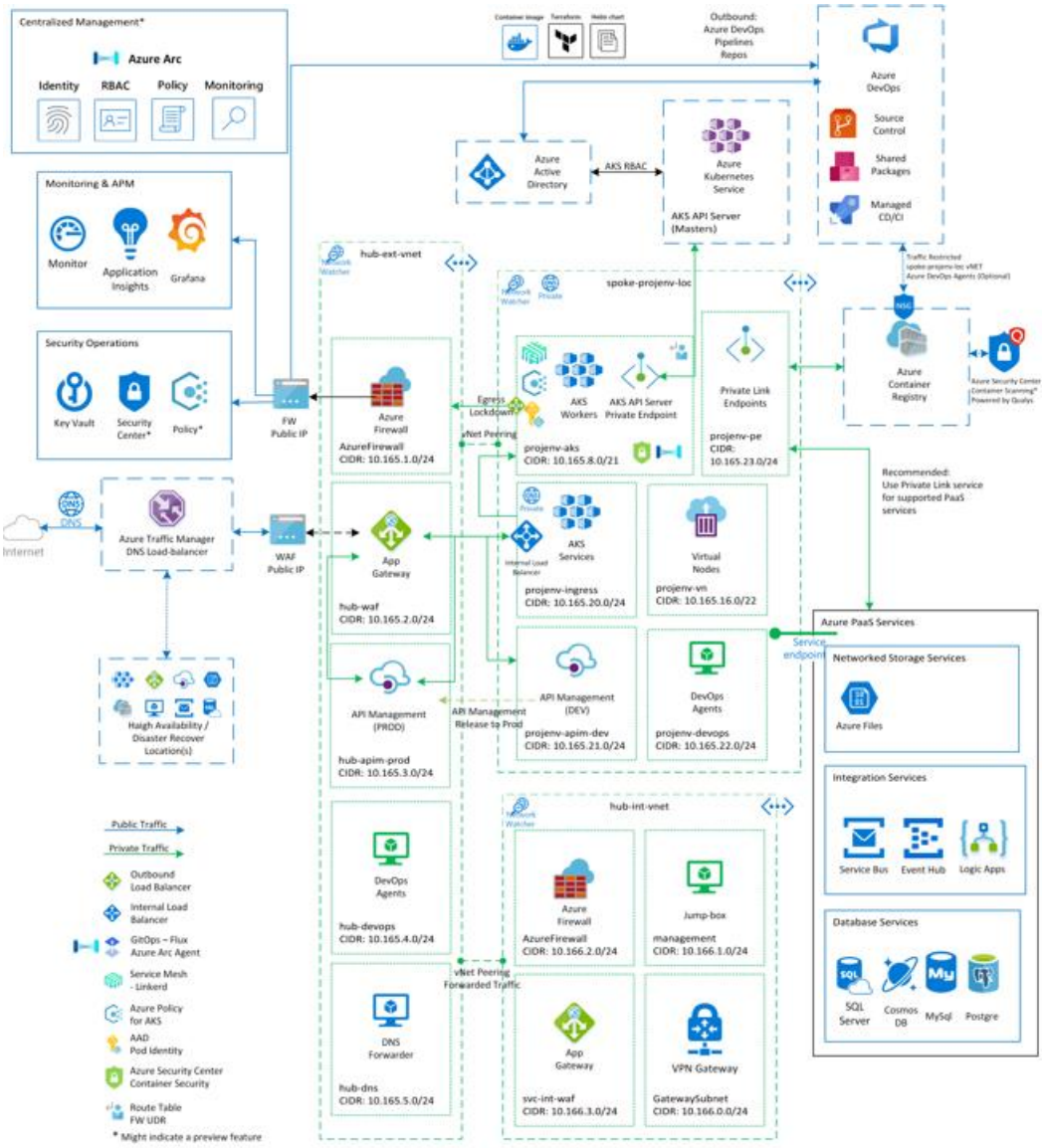
3.5.6 Audit Trail and History

The system maintains a complete log of all actions taken on an application — submissions, updates, verifications, and communications. This audit trail enhances accountability and provides a reliable record for dispute resolution.

3.6 Technical Delivery Approach (Microservices + Event-Driven Modernisation)



We will enhance and modernise the existing platform using a **microservices-based redevelopment approach** (incremental modularisation) and **event-driven patterns** to improve scalability, maintainability, and change isolation—while operating within the GDE-owned Azure environment and governance requirements.

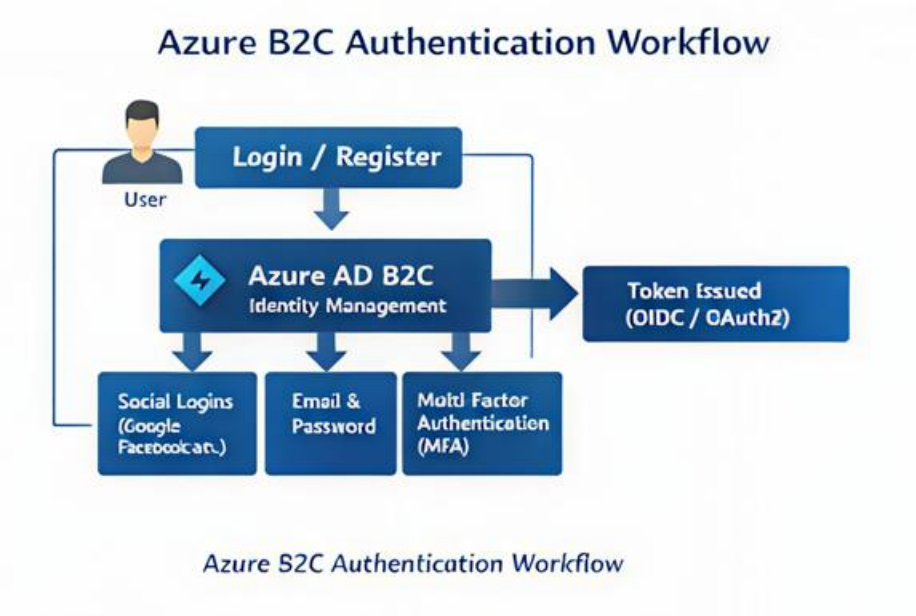


This supports the TOR's requirements for:

- Scalability and performance for **60,000+ concurrent users**.
- Maintainability and supportability through controlled enhancements over 36 months.
- Strong auditability and traceability through consistent system event logging and controlled changes

Note: The TOR explicitly excludes unapproved enhancements and expects changes to be aligned to approved requirements/change control; we will apply microservices modularisation in a controlled, incremental manner governed by the BRS/FRS and formal change authorisation.

3.7 Identity, Access and Security (Azure AD B2C + RBAC + Audit)



Azure B2C Authentication Workflow

- **Azure AD B2C** will be used for secure user registration and authentication for citizen users (parents/guardians), with secure token-based access to the platform.
- **RBAC** will enforce least privilege across user groups (parents, schools, district, provincial, special-schools stakeholders), supporting segregation of duties.

This aligns with TOR requirements to implement:

- Secure registration/authentication and **role-based access control (RBAC)**.

- Comprehensive and exportable audit trails and activity logging.
- Security controls aligned to MISS and POPIA and security monitoring/logging enabled.

Auditability approach:

- User access events, workflow decisions, administrative actions, and data changes; logs are retained and exportable for oversight and investigations.

3.8 Workflow Automation (Power Automate-driven process orchestration)

We will implement admissions workflow orchestration using **Power Automate** for human approvals, escalations, and routing (where appropriate), while maintaining system-of-record state in the admissions platform.

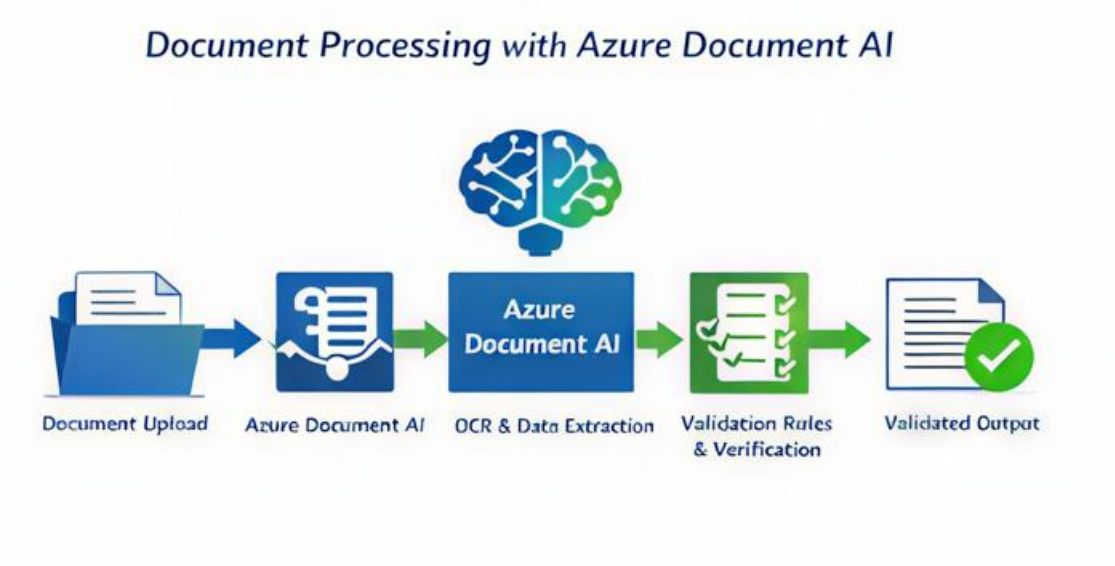
This directly supports TOR requirements for:

- Workflow routing through defined stages (school → district → provincial), including escalations and approvals
- Automated notifications via SMS/email at specific process stages.
- Operational controls that reduce manual processing and improve turnaround times.

Each workflow execution will be captured as part of the audit evidence pack to support traceability and compliance

3.9 Document Validation (Azure Document AI)

Documents uploaded by applicants will be validated using **Azure Document AI** to extract key fields (OCR + structured extraction) and validate them against defined rules and completeness checks, routing exceptions to manual review queues.



This strengthens:

- Operational efficiency during peak periods,
- Consistency of document verification,
- Audit-ready evidence of verification outcomes.

This aligns with the TOR's emphasis on controlled processes, automation, and governance of the application lifecycle and supporting evidence

3.10 Testing, Quality Assurance & Performance Readiness

All enhancements and modules will undergo the TOR-required testing lifecycle:

- Functional testing, regression testing, performance/stress testing, and UAT.
- Defects found during any phase (including UAT) are resolved prior to production.
- Test artefacts/results are documented and retained for review and audit.

Performance readiness specifically targets the TOR requirement for **60,000+ concurrent users**, supported by documented performance testing and optimisations.

3.11 Release Management & Operational Safety

We will deploy changes using controlled release processes:

- Releases aligned to agreed deployment windows and admissions operational constraints.
- Rollback procedures maintained for each production release to mitigate risk.
- No changes will be introduced that jeopardise availability during critical admissions windows.

3.12 Support & Maintenance Approach (36 months)

Support is delivered as an operational workstream across the full contract:

- SLA-based incident support and proactive maintenance, including peak-period support coverage as defined in SLA.
- Scheduled meetings and reporting (weekly/fortnightly/monthly/quarterly and ad hoc) with operational metrics, uptime, and resolution timelines.
- Preventive maintenance, patching, performance optimisation, and security fixes as required

3.13 Skills Transfer & Sustainability

Skills transfer is executed from inception through to close-out and includes:

- Formal and hands-on training, mentoring, train-the-trainer approaches, and artefact handover
- Mandatory knowledge artefacts: architecture documentation, configuration/deployment guides, SOPs, security and audit procedures, and DR/backup procedures
- Formal handover milestone with signed checklist and demonstrated capability for GDE to operate the system independently.

4 Project Plan

4.1 Year 1 — Week-by-Week Timeline (W1–W8) Go-Live within 2 Months

Week	Timeline	TOR Milestone Alignment	Planned Activities (timeboxed)
W1	Week 1	**Milestone 1: Project Inception & Mobilization**	Contract kick-off; governance structures; confirm project plan & risk register; agree milestone acceptance criteria
W2	Week 2	**Milestone 2: Requirements Validation & Detailed Design**	Validate existing platform requirements; confirm Grade R + Grade 1/8 enhancements; baseline delivery schedule aligned to admissions calendar
W3	Week 3	**Milestone 2 (continued)**	Updated solution architecture (baseline); confirm RBAC/audit/logging expectations; baseline test approach and reporting cadence
W4	Week 4	**Milestone 3: System Enhancements & New Functionality**	Start build/config: enhancements to existing admissions modules; begin Grade R module implementation; integration updates (where applicable) and configuration aligned to policies
W5	Week 5	**Milestone 3 (continued)**	Continue build/config: Grade R module; configuration aligned to policies; prepare test-ready increment
W6	Week 6	**Testing, UAT & Operational Readiness**	Functional testing + regression testing + performance testing preparation; defect fixing loop
W7	Week 7	**Testing, UAT & Operational Readiness**	Execute UAT with stakeholders; address defects; pre-go-live stabilisation
W8	Week 8	**Admissions Go-Live (within 2 Months)**	Controlled system opening; hypercare/stabilisation support; performance monitoring during peak load

4.2 (M1–M36) — Aligned to Milestones 1–10

4.2.1 Master Gantt (Milestones Only)

TOR Milestone	Name (as per TOR indicators)	Start	End
M1	Project Inception & Mobilization	M1	M1
M2	Requirements Validation & Detailed Design	M1	M2
M3	System Enhancements & New Functionality (Year 1)	M2	M3
(Embedded)	Testing, UAT & Operational Readiness (Year 1)	M2	M3
(Embedded)	Admissions Go-Live (within 2 Months)	M2	M3
M4	Support & Maintenance (Year 1, as-and-when)	M3	M12
M5	System Enhancements & New Functionality for Year 2 (Validation & Plan)	M10	M13
M6	System Enhancements & New Functionality for Year 2 (UAT & Readiness)	M15	M18
M7	Support & Maintenance (Year 2, as-and-when)	M13	M24
M8	System Enhancements & New Functionality for Year 3 (Validation & Plan)	M22	M25
M9	System Enhancements & New Functionality for Year 3 (UAT & Readiness)	M27	M31
M10	Support & Maintenance (Year 3) + Formal Handover	M25	M36

4.3 Detailed Month-by-Month Workplan

4.3.1 Year 1 (M1–M12)

Work Package (TOR Indicator)	Detailed Timeline	Start	End
Milestone 1: Project Inception & Mobilization	Contract kick-off; governance structures; confirmed project plan & risk register; agreed milestone acceptance criteria	M1	M1
Milestone 2: Requirements Validation & Detailed Design	Validate existing platform requirements; confirm Grade R + Grade 1/8 enhancements; updated architecture; finalised delivery schedule aligned to admissions calendar	M1	M2
Milestone 3: System Enhancements & New Functionality (Year 1)	Enhancements to existing admissions modules; Grade R module development & implementation; integration updates (where applicable); configuration aligned to policies	M2	M3

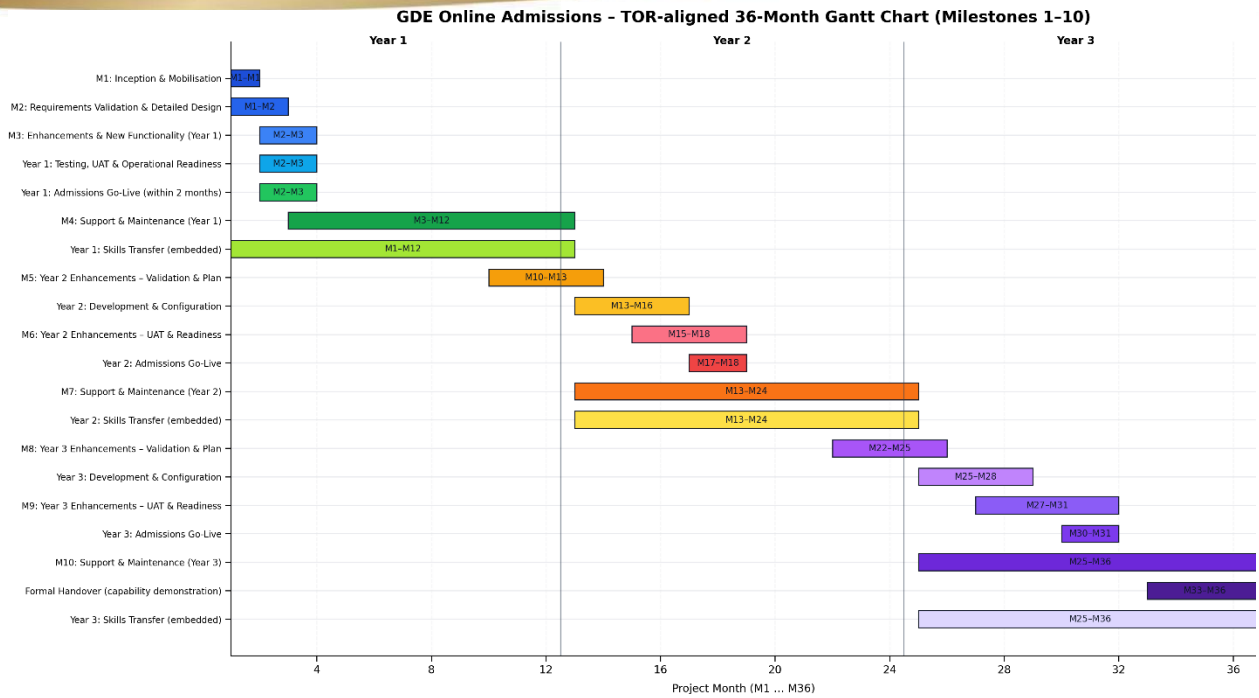
Testing, UAT & Operational Readiness (Year 1)	Functional, regression, performance testing; UAT; pre-go-live stabilisation	M2	M3
Admissions Go-Live (within 2 Months)	Controlled system opening; hypercare/stabilisation support; performance monitoring during peak load	M2	M3
Milestone 4: Support & Maintenance (Year 1, As-and-when)	SLA-based incident support (L2/L3); scheduled maintenance (quarterly/bi-annual); performance & health reporting; preventive maintenance	M3	M12
Skills Transfer & Formal Handover (embedded in Year 1)	Training delivery (train-the-trainer); system support during training; documentation & SOPs; knowledge artefacts	M1	M12

4.3.2 Year 2 (M13–M24)

Work Package (TOR Indicator)	Detailed Timeline	Start	End
Milestone 5: System Enhancements & New Functionality for Year 2 (Validation & Plan)	Validation of existing requirements; confirmation of enhancements; updated solution architecture; finalised delivery schedule aligned to admissions calendar	M10	M13
Development & Configuration (Year 2 delivery)	Enhancements to existing admissions modules; module implementation; integration updates (where applicable); configuration aligned to policies	M13	M16
Testing, UAT & Operational Readiness (Year 2)	Functional, regression, performance testing; UAT; pre-go-live stabilisation	M15	M18
Milestone 6: Enhancements for Year 2 (UAT + Stabilisation)	UAT and go-live readiness completion	M15	M18
Admissions Go-Live (Year 2)	Controlled system opening; hypercare/stabilisation support	M17	M18
Milestone 7: Support & Maintenance (Year 2, As-and-when)	SLA-based incident support; scheduled maintenance; performance & health reporting; preventive maintenance	M13	M24
Skills Transfer & Formal Handover (embedded in Year 2)	Training delivery; documentation & SOP updates; knowledge artefacts refresh	M13	M24

4.3.3 Year 3 (M25–M36)

Work Package (TOR Indicator)	Detailed Timeline	Start	End
Milestone 8: System Enhancements & New Functionality for Year 3 (Validation & Plan)	Validation of existing requirements; confirmation of enhancements; updated architecture; finalised delivery schedule aligned to admissions calendar	M22	M25
Development & Configuration (Year 3 delivery)	Enhancements to existing admissions modules; module implementation; integration updates (where applicable); configuration aligned to policies	M25	M28
Testing, UAT & Operational Readiness (Year 3)	Functional, regression, performance testing; UAT; pre-go-live stabilisation	M27	M31
Milestone 9: Enhancements for Year 3 (UAT + Stabilisation)	UAT and go-live readiness completion	M27	M31
Admissions Go-Live (Year 3)	Controlled system opening; hypercare/stabilisation support	M30	M31
Milestone 10: Support & Maintenance (Year 3)	SLA-based incident support; scheduled maintenance; performance & health reporting; preventive maintenance	M25	M36
Formal Handover (end-state)	Demonstrated capability for GDE to operate system independently (formal handover indicator)	M33	M36
Skills Transfer & Formal Handover (embedded in Year 3)	Training delivery; documentation & SOPs; knowledge artefacts; close-out handover activities	M25	M36



5 Service Scope & Service Catalogue

5.1 In-Scope Service Components

- Application Support (L1/L2/L3): incident management, investigation, resolution, and stakeholder communication.
- Preventative Maintenance: planned patch coordination, dependency upgrades, housekeeping, and configuration hygiene.
- Corrective Maintenance: defect fixes, minor enhancements, and regression prevention.
- Operational Monitoring: 24x7 critical alerting for Sev 1 conditions and defined monitoring coverage for Sev 2–4.
- Release Management: monthly releases, emergency hotfixes, CAB documentation, and post-release validation.
- Security Operations Support: vulnerability triage and remediation coordination within release cycles.
- Modernisation Delivery: microservices decomposition and platform improvement work packages.
- AI Enablement Delivery: design, pilot, productionisation, and monitoring of approved AI capabilities.

5.2 Service Catalogue

Service Area	Activities	Outputs	Cadence
Service Desk & Intake	Ticket intake, triage, routing, comms	Ticket records, comms updates	Daily
Incident Management	Restore service, workarounds, PIR	Resolved incidents, PIR notes	As required
Problem Management	RCA, trends, KEDB	RCA reports, known error entries	Monthly
Change & Release	CAB, deploy, rollback	Release notes, change records	Monthly/Ad hoc
Monitoring & Observability	Dashboards, alerts, tuning	Dashboards, alert policies	Continuous
Performance Engineering	Load tests, tuning	Test results, tuning actions	Pre-peak + Quarterly
Security Support	Vuln remediation planning	Remediation actions, evidence	Monthly
Enhancements	Minor improvements	Delivered features/fixes	Sprint-based

5.3 Maintenance Types

- Corrective maintenance: defect fixes to restore expected behaviour.
- Adaptive maintenance: changes required due to external changes (policy rules, integration changes, platform updates).
- Perfective maintenance: improvements to usability, performance, and maintainability.
- Preventative maintenance: proactive actions to reduce risk (patch planning, dependency up-dates, refactoring hotspots).

5.4 Service Request Types

- Configuration changes (feature toggles, rule parameters) under change control.
- Content updates (announcements, FAQs, guidance text) where portal supports CMS/config.
- Data correction requests (subject to governance and approvals).
- Report extracts and operational data requests (subject to privacy and access controls).

6 Service Levels (SLA), KPIs & Reporting

6.1 Severity Definitions

- Severity 1 (Critical): Portal unavailable or major data/security incident with significant public impact.
- Severity 2 (High): Major function impaired affecting large user groups; no viable workaround.
- Severity 3 (Medium): Partial degradation or limited impact with workaround available.
- Severity 4 (Low): Minor defect or service request with minimal impact.

6.2 SLA Targets (Baseline)

Severity	Response Target	Restore Target	Update Frequency	Ownership
Sev 1	30 minutes	4 hours	Every 60 minutes until restore	Rifumo with Client escalation
Sev 2	1 hour	16 hours	Every 4 hours	Rifumo
Sev 3	4 hours	5 business days	Every 2 business days	Rifumo
Sev 4	1 business day	Planned release	Weekly	Rifumo

6.3 Support Hours & Coverage

- Business hours coverage: 08:00–17:00 (Mon–Fri) for Sev 2–4 and service requests.
- 24x7 on-call: Sev 1 incidents year-round.
- Peak admissions extended coverage: 06:00–22:00 including weekends during defined admissions windows (planned annually).

6.4 Service KPIs (Measured Monthly)

- SLA compliance (% incidents meeting response and restoration targets).
- Mean Time to Restore (MTTR) by severity.
- Incident recurrence rate (repeat incidents within 30 days).
- Change success rate (deployments without Sev 1/2 incidents caused by change).
- Deployment frequency and lead time for change.
- Portal performance KPIs (p95 response time for key journeys; error rates).
- Availability during admissions windows (uptime and major degradation minutes).

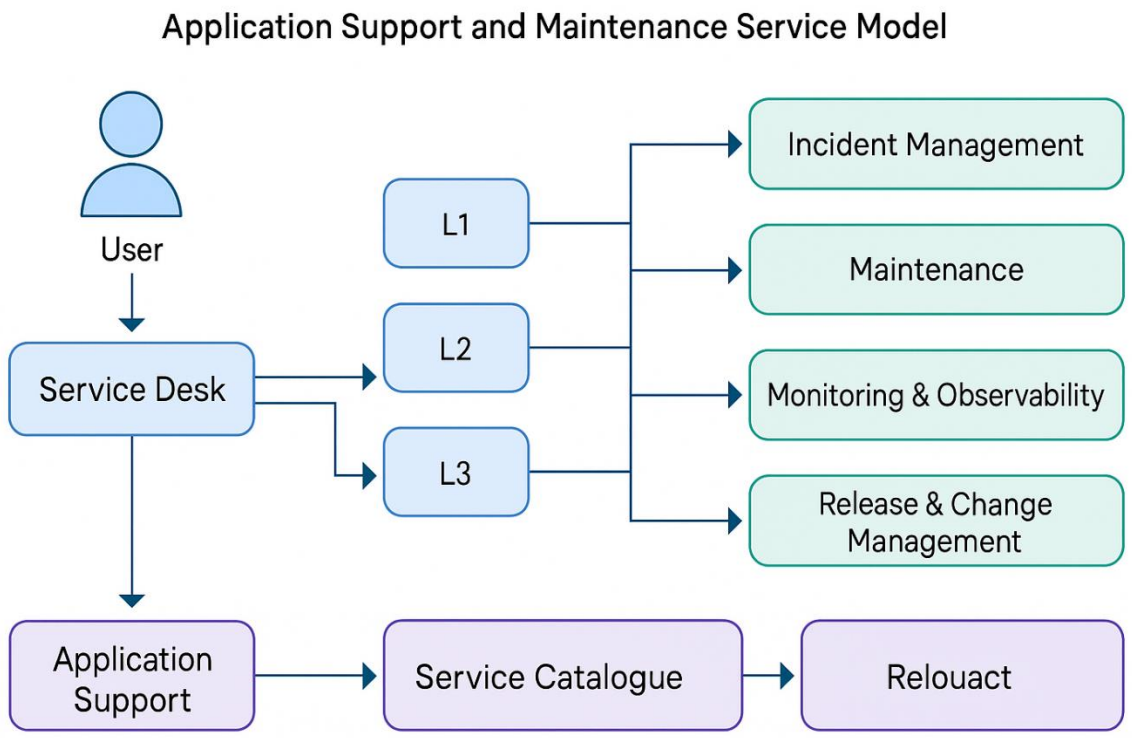
6.5 Reporting

- Weekly operational report: incidents, changes, backlog, risks, and planned work.
- Monthly service report: SLA/KPI performance, trends, RCAs, improvements delivered, and next-month plan.
- Quarterly executive report: roadmap progress, modernisation outcomes, AI adoption metrics, and value delivered.

7 Operating Model, Governance & RACI

7.1 Governance Structure

- Operational Working Group (Weekly): service manager, technical lead, client operations representative.
- Change Advisory Board (As required): reviews planned changes, risk, and deployment windows.
- Service Review (Monthly): SLA/KPI review, backlog prioritisation, major risks and decisions.
- Steering Committee (Quarterly): strategy, budget, policy implications, and escalations.



7.2 Escalation Path

- Level 1: Service Desk / Support Lead
- Level 2: Technical Lead / SRE
- Level 3: Solution Architect / Service Delivery Manager
- Executive escalation: Account Executive / Client Sponsor

7.3 RACI

Activity	Rifumo	GDE ICT	GDE Business	3rd Parties/Integrations
Incident resolution	R	C	I	C
Major change approval	C	R	R	C
Release deployment	R	C	I	C
UAT sign-off	C	I	R	I
Security audit evidence	R	R	I	C

Legend: R=Responsible, A=Accountable, C=Consulted, I=Informed. Full RACI is provided in Appendix A.

8 Technical Approach: Stabilisation, Maintenance & Performance Engineering

8.1 Transition-In (Mobilisation) Activities

- Access provisioning: source repositories, CI/CD pipelines, environments, monitoring tools, and ticketing systems.
- Knowledge transfer: architecture walkthroughs, operational runbooks, known issues, and release history.
- Baseline assessment: availability, performance, error rates, and security posture (high-level).
- Support process alignment: severity definitions, comms templates, escalation matrix, and CAB approach.
- Initial backlog triage: categorise defects, technical debt, and enhancement requests.

8.2 Observability Uplift

- Implement/standardise logging, metrics and distributed tracing (where feasible).
- Define SLOs for critical user journeys (login, application submission, document upload, status check).
- Create dashboards for business and technical stakeholders (health, volume, errors, performance).
- Establish alert policies (thresholds, anomaly alerts) and runbooks per alert.

8.3 Performance Engineering & Peak Readiness

- Define peak load scenarios and workload models (concurrent users, transaction mix, upload patterns).
- Conduct load and stress tests ahead of admissions windows; identify bottlenecks.
- Implement performance improvements: caching, query optimisation, async processing, scaling rules.
- Run “go/no-go” readiness checklist prior to peak: capacity, monitoring, rollback, comms plan.

8.4 Maintenance & Technical Debt Management

- Maintain a technical debt register with prioritised remediation items.
- Schedule monthly maintenance windows for patching and dependency updates (subject to CAB).
- Use automated regression tests to validate fixes and prevent re-introduction of defects.
- Implement coding standards and architecture guardrails to reduce future debt.

9 Modernisation Programme: Microservices Decoupling

9.1 Approach (Incremental Strangler Pattern)

Modernisation will be delivered incrementally to avoid disruption. New microservices will be introduced behind an API gateway, with routing progressively shifted from the legacy core. Where appropriate, event-driven patterns will be introduced to decouple workflows.

9.2 Domain Decomposition (Illustrative)

- Identity & Access Service (integration with identity provider and role model).
- Applicant Profile Service (parent/guardian and learner profiles).
- Applications Service (submission, validation orchestration, rule evaluation).
- Documents Service (upload, storage orchestration, metadata, virus scanning integration).
- Notifications Service (SMS/email templates, send policies, retries, audit).
- Placement Service (allocation workflow, capacity checks, offers/acceptance).
- Appeals Service (case management, evidence, workflow).
- Reporting Service (operational reports, extracts, dashboards).

9.3 Technical Patterns & Standards

- API-first: OpenAPI specifications, versioning, and backward compatibility policy.
- Event-driven workflows: publish domain events; use queues/topics for reliable async processing.
- Service data ownership: each service owns its datastore; cross-service queries via APIs/events.
- Resilience: retries with backoff, circuit breakers, idempotency keys, dead-letter handling.
- Security: OAuth2/OIDC, service-to-service identity, secrets management, least privilege.
- Observability: consistent correlation IDs, structured logging, traces, and health probes.

9.4 Modernisation Waves (36 months)

Wave	Target Period	Scope (Illustrative)	Deliverables
Wave 1	Months 3–12	Low-risk extraction: Notifications, Documents metadata, Read-only APIs	Services deployed, API gateway routes, monitoring, runbooks
Wave 2	Months 13–24	Core journey extraction: Applicant Profile,	Services + eventing, contract

		Application Submission, Validation Rules	tests, regression suite
Wave 3	Months 25–36	High-value workflows: Placement, Appeals, Reporting services	Legacy retirement plan, data migration steps, performance improvements

9.5 Deliverables (Microservices)

- Target reference architecture and standards pack (APIs, events, security, observability).
- Service definitions (bounded contexts), API specifications and event schemas.
- CI/CD pipelines for each service with automated testing and security scanning.
- Operational runbooks, dashboards and alerts per service.
- Incremental routing and cutover plan with rollback procedures.
- Legacy component retirement plan (where replaced).

10 Security, Privacy (POPIA) & Compliance

10.1 Security Controls

- Identity and access management: least privilege, role separation, and MFA for privileged accounts.
- Encryption: TLS for data in transit; encryption at rest for databases and storage.
- Secure secrets management: centralised secret store and rotation procedures.
- Vulnerability management: dependency scanning, SAST/DAST where feasible, and patch planning.
- Audit logging: immutable logs for admin actions and critical workflow events.
- Web protections: WAF and DDoS protections where available in hosting environment.

10.2 POPIA Alignment (Operational Controls)

- Purpose limitation and lawful processing for all personal information.
- Data retention and deletion policies aligned to business and legal requirements.
- Access reviews and segregation of duties for administrators.
- Incident response process including potential breach notification procedures as per Client governance.
- Privacy impact assessments for AI use cases that process personal information.

10.3 Compliance Evidence & Audit Support

- Maintain evidence packs for changes, deployments, approvals and test results.
- Provide monthly vulnerability remediation status and security improvement actions.
- Support audit requests with logs, change records and control evidence (subject to access).

11 Business Continuity, DR & Resilience

11.1 Continuity Objectives

- Define and maintain RTO/RPO targets per critical component (to be finalised with Client).
- Ensure backup schedules and restore tests are performed and evidenced.
- Document failover procedures and execute DR drills twice per year.

11.2 DR Drill Plan

1. Plan: agree DR scenario, scope, success criteria and communications.
2. Execute: failover simulation (where supported) or restore-based recovery test.
3. Validate: confirm portal journeys, integrations, and data consistency checks.
4. Report: document outcomes, issues, and remediation backlog.

11.3 Resilience Patterns

- Stateless service scaling for web/API components where feasible.
- Queue-based buffering for asynchronous operations (notifications, document processing).
- Graceful degradation for non-critical features during peak.
- Rate limiting and backpressure via API gateway.

12 Tooling, DevSecOps & Quality Engineering

12.1 DevSecOps

- CI/CD pipelines with automated build, test, security scans, and deployment approvals.
- Infrastructure as Code (IaC) for reproducible environments (where applicable).
- Branching strategy and release tagging to ensure traceability.

12.2 Testing Strategy

- Automated unit tests and service contract tests for microservices.
- Automated regression tests for critical portal journeys.
- Performance tests and soak tests ahead of admissions windows.
- Security tests (dependency checks, SAST/DAST where feasible).
- UAT support and defect triage with clear acceptance criteria.

12.3 Documentation & Runbooks

- Operational runbooks per major component/service with step-by-step resolution paths.
- Architecture and integration documentation updated quarterly.
- Knowledge base content for common issues and user guidance.

13 Resource Plan & Team Structure

13.1 Team Model

- Service Delivery Manager: overall governance, reporting, stakeholder management.
- Solution Architect: design authority, standards, and microservices roadmap ownership.
- Technical Lead: engineering leadership and complex issue resolution.
- Support Engineers (L2): triage, investigation, standard fixes and operational execution.
- Software Engineers (L3): code-level fixes, enhancements and microservices delivery.
- SRE/DevOps: CI/CD, reliability engineering, monitoring and environment operations.
- QA/Test Automation: automated regression and release quality gates.
- Data/AI Engineer: AI delivery and analytics; MLOps governance.
- Security Specialist (shared): security reviews, vulnerability planning and audit support.

13.2 Skills Transfer

- Quarterly knowledge transfer sessions with client ICT and operational stakeholders.
- Documentation handover and runbook updates on each major release.
- Shadow-to-lead transition approach for critical operational activities.

14 Risk Management & Mitigation

Risk	Description	Mitigation
Peak load instability	Admissions peaks may exceed capacity causing slowdowns or outages.	Pre-peak load testing, tuning sprints, autoscaling readiness, caching and synthetic monitoring.
Legacy coupling	Tight coupling increases change risk and lead time.	Strangler approach, API façade, event-driven integration and incremental service extraction.
Integration dependency changes	Upstream/downstream changes impact portal flows.	Versioned contracts, integration monitoring, joint testing windows, and escalation paths.
Security and privacy	PII exposure risk, particularly with AI capabilities.	POPIA-aligned controls, redaction/minimisation, RBAC, auditing, and human-in-the-loop.
Change volume	Policy/rule changes create backlog pressure.	Quarterly roadmap planning, prioritisation workshops, and strict change control.

15 Dependencies, Assumptions & Client Obligations

15.1 Dependencies

- Timely access to source code repositories, environments, logs and CI/CD pipelines.
- Availability of Client stakeholders for backlog prioritisation, UAT and approvals.
- Timely CAB and security approvals for production changes.
- Availability of integration owners and third parties for interface validation.

15.2 Assumptions

- All costs are VAT inclusive as per the Pricing Schedule (SBD 3.3).
- Third-party licensing and hosting consumption (compute/storage/AI platform consumption) are excluded unless explicitly contracted.
- AI use cases are implemented only after approval of data governance and privacy controls.
- Scope is governed through the agreed backlog and change control process; materially new scope requires a variation order.

15.3 Client Obligations

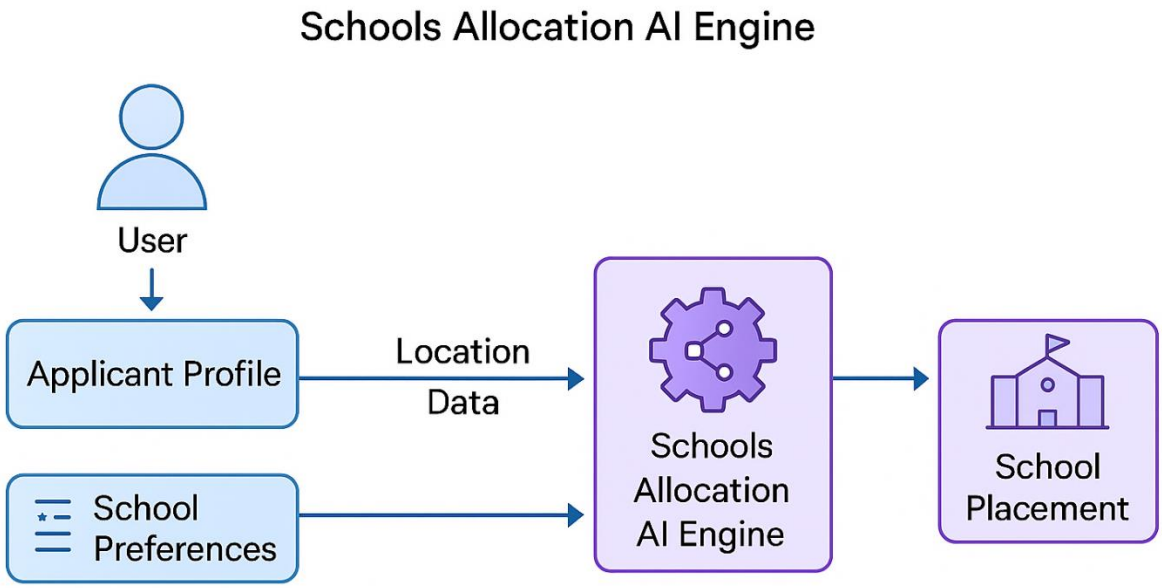
- Provide timely access and credentials, including security approvals for tooling.
- Assign product owner/service owner and SMEs for requirements and UAT.
- Provide policy/rule definitions and change notices for admissions process updates.
- Provide incident communication channels and participate in major incident reviews.

16 Out of Scope

- Replacement of the Portal with a completely new product outside the agreed modernisation roadmap.
- Large-scale data cleansing beyond agreed validation and transformation rules.
- End-user device procurement and support.
- Unbounded feature development not prioritised through governance and backlog management.
- Cloud platform consumption overages and third-party licensing unless explicitly included.

17 AI Enablement Programme and Innovation

The below is not in current scope this is some of the ideas we have a partner that can lead the GDE into the AI Age. We can engage later on what can be done with AI in the education space.



17.1 AI Use Case Roadmap

Use Case	Value	Delivery Stage	Target Period
Admissions Virtual Assistant	Reduces queries; improves self-service	Pilot → Production	Months 3–12 (pilot), Months 13–18 (production)
Operational Copilot for Admin/Contact Centre	Faster case handling and summarisation	Pilot → Production	Months 9–18
Demand/Capacity Forecasting	Improves peak readiness and scaling	Pilot → Production	Months 13–24
Anomaly/Fraud Signal Detection	Supports integrity and governance	Pilot → Production	Months 18–36
Document Intelligence (classification/completeness)	Reduces manual review	Pilot (policy dependent)	Months 13–36

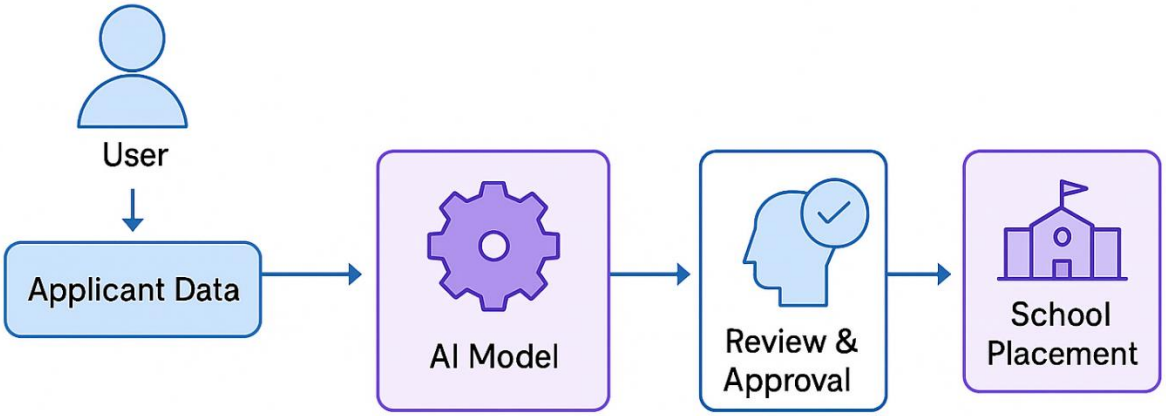
17.2 Responsible AI & Governance Controls

- Data minimisation: only use necessary fields; avoid unnecessary retention of PII.
- Security and access control: enforce RBAC and audit trails for AI-assisted workflows.
- Human-in-the-loop: AI outputs are advisory; high-impact decisions remain with authorised officials.
- Model monitoring: track accuracy, drift, and error patterns; periodic re-validation.
- Content safeguards: prompt controls, toxicity filters where available, and escalation to human agents.
- Transparency: user-facing messaging that AI assistance is provided and how to escalate.

17.3 AI Architecture (High-Level)

- AI service layer integrated via APIs with the portal and support tooling.
- Knowledge base curated from approved content (FAQs, policy docs, process guidance).
- Analytics pipeline for telemetry and adoption metrics (deflection rate, satisfaction, resolution time).
- MLOps pipeline for model lifecycle management (when training/custom models are approved).

AI Decision Governance



Appendix B: Service Catalogue (Detailed)

A1. Incident Management – Detailed Steps

5. Detection/Logging: ticket created via service desk, monitoring alert, or stakeholder notification.
6. Classification: assign severity, impacted service/component, and initial hypothesis.
7. Triage: collect logs, telemetry, reproduction steps; assign to appropriate resolver group.
8. Containment: implement workaround (if available) to restore service quickly.
9. Resolution: deliver fix via change process; validate and monitor stability.
10. Post-Incident Review: for Sev 1/2, complete PIR including root cause, timeline, and prevention actions.

A2. Problem Management – Detailed Outputs

- Monthly trend analysis: top incident categories, recurring faults, and ageing problems.
- Root Cause Analysis (RCA) documents for material incidents, including contributing factors.
- Known Error Database (KEDB) entries: symptoms, workarounds, permanent fix reference.
- Prevention backlog: prioritised technical debt or refactoring tasks tied to incident reduction.

A3. Change & Release Management – Detailed Steps

11. Request: change logged with description, scope, risk, and proposed window.
12. Assessment: technical review, security review (where relevant), and testing plan defined.
13. Approval: CAB approval based on risk and business impact.
14. Implementation: deploy via CI/CD pipeline with version tagging and evidence capture.
15. Validation: smoke tests and key journey checks; monitoring for anomalies.
16. Closure: update change record with outcomes and evidence; publish release notes.

A4. Service Request Fulfilment

- Requests are logged and categorised; standard requests follow predefined workflows and approvals.
- Non-standard requests follow analysis and change control if they affect production behaviour.
- Turnaround times depend on request complexity and prioritisation in the backlog.

Appendix B: SLA Matrix, Severity Definitions & Escalation

B1. Severity Decision Guide

- Classify as Sev 1 if the Portal is unavailable, data integrity is at risk, or a security incident is suspected.
- Classify as Sev 2 if a major user journey fails for many users with no workaround.
- Classify as Sev 3 if limited subset is impacted or workaround exists.
- Classify as Sev 4 for minor issues and requests.

B2. Communication Templates (Summary)

- Major Incident Notification: impact, start time, affected services, workaround, next update time.
- Status Update: investigation progress, ETA, risks, next update time.
- Resolution Notice: restored time, root cause summary, next steps and PIR schedule.

Appendix C: Sample Monthly Service Report (Template)

C1. Executive Summary

- Overall SLA performance (month-to-date).
- Key incidents and outcomes.
- Changes and releases delivered.
- Modernisation and AI progress highlights.
- Key risks and decisions required.

C2. SLA & KPI Dashboard (Headings)

- SLA compliance by severity
- MTTR trend
- Incident volume and categories
- Change success rate
- Performance KPIs (p95, error rate)
- Availability (peak window vs normal)

C3. Backlog & Delivery

- Top 10 backlog items delivered (defects/enhancements).
- Modernisation epics progress and completed deliverables.
- AI use case metrics (adoption, deflection, satisfaction).

Appendix D: Modernisation Backlog (Illustrative Epics)

- Epic D1: API Gateway implementation and API standardisation (versioning, throttling, analytics).
- Epic D2: Notifications service extraction (templating, auditing, retries, DLQ).
- Epic D3: Document service hardening (upload pipeline, virus scanning integration, metadata store).
- Epic D4: Application submission service extraction (validation orchestration, rule engine integration).
- Epic D5: Applicant profile service extraction (master data ownership and validation).
- Epic D6: Placement workflow service (allocation, capacity, offers, acceptance).
- Epic D7: Appeals case management service (workflow and evidence handling).
- Epic D8: Reporting service decoupling (operational extracts, dashboards).

Appendix E: AI Use Case Catalogue & Responsible AI Controls

E1. Use Case Details – Virtual Assistant

- Channels: Portal web chat; optional WhatsApp/MS Teams integration for internal users.
- Knowledge sources: approved FAQs, process guides, policy extracts, and operational announcements.
- Analytics: deflection rate, conversation success, escalation volume, and user feedback scores.
- Controls: PII redaction where feasible, guardrails on policy advice, escalation to human support.

E2. Use Case Details – Operational Copilot

- Summarises cases and highlights missing information to reduce handling time.
- Provides consistent guidance based on approved policy and SOPs.
- Includes audit logging of AI suggestions shown to users.

E3. Risk Controls

- No automated final decisioning: AI outputs are advisory.
- Access restrictions: only authorised roles can view sensitive AI outputs.
- Monitoring: regular review of AI responses for correctness and bias risks.
- Escalation: human override and reporting channels for problematic outputs.

Appendix G: Glossary & Acronyms

Term	Definition
AI	Artificial Intelligence
API	Application Programming Interface
CAB	Change Advisory Board
CI/CD	Continuous Integration / Continuous Deployment
DR	Disaster Recovery
KEDB	Known Error Database
MTTR	Mean Time To Restore
POPIA	Protection of Personal Information Act (South Africa)
RACI	Responsible, Accountable, Consulted, Informed
RCA	Root Cause Analysis
SLA	Service Level Agreement
SLO	Service Level Objective
SRE	Site Reliability Engineering