Microsoft 365 Agents SDK and Copilot Extensions

Course code: SPO_COPILOT

The course focuses on the design, development, validation, and operation of agents built on Microsoft 365 Agents SDK and Copilot Extensions. Emphasis on multi-channel deployment (Copilot, Teams, web), activity processing, action handlers, secure data anchoring (SharePoint/Graph), Responsible AI, evaluation telemetry, and lifecycle using Microsoft 365 Agents Toolkit and Agents Playground.

Who is this course for

- Solution architects and AI engineers
- Microsoft 365 developers extending Copilot
- Technology consultants designing enterprise AI integrations
- Platform engineers enabling secure AI adoption

Required prerequisites

- C# basics at the level of the GOC2125 course
- JavaScript basics at the JS_PROG1 course level
- TypeScript basics at the JS_TS1 course level
- Knowledge of REST &JSON
- Azure &Microsoft 365 basics
- Previous work with Microsoft Graph (optional/advantageous)
- Experience with prompt engineering (optional/advantageous)

Course outline

- Copilot architecture &Agents SDK overview (2 hours)
- Extension options: Agents SDK, plugins, Graph connectors, actions
- Azure Bot Service channels and adapters; activities and "turns"
- Microsoft 365 Agents Toolkit &Playground (2.5 hours)
- Templates for Visual Studio/VS Code, scaffolding, local Agents Playground
- Supported languages (C#, JS/Node, Python) and prerequisites
- Responsible AI &governance (2.5 hours)
- Guardrails, safety filters, content moderation
- Privacy, compliance &traceability
- Corporate ingestion strategy (2.5 hours)
- Principles of SharePoint/OneDrive content indexing
- Graph connectors &metadata enrichment
- Vectorization &RAG design (2.5 hours)
- Chunking, embeddings, hybrid semantic ranking
- Latency vs. relevance trade-offs
- Prompt &system orchestration (2.5 hours)
- System vs. user vs. tool messages
- Few-shot, prompt chaining, evaluation heuristics
- Application agent, manifest &API surface (2.5 hours)
- AgentApplication/AgentApplicationOptions basics; endpoint mapping
- Manifest, capability declarations, versioning
- Action handlers &integration with Microsoft Graph (2.5 hours)
- Action routing
- Parameter validation
- Permission boundaries
- Middleware &enforcement policies (2.5 hours)

GOPAS®

- Pre/post processing, editing, output filtering
- Hallucination mitigation patterns
- Event-driven orchestration (2.5 hours)
- Azure Functions vs Logic Apps vs Durable orchestrations
- Model and tool call chaining
- Evaluation &quality (2.5 hours)
- Qualitative vs quantitative metrics, human-in-the-loop
- Golden set &regression tests
- Performance, costs &scaling (2.5 hours)
- Token economy, cache layers, retrieval optimization
- Resilience and timeout patterns
- Security &risk management (2.5 hours)
- Exfiltration prevention, scope minimization
- Output sanitization and watermarking (where appropriate)
- Deployment &lifecycle management (2.5 hours)
- Propagation between environments, versioning, rollback
- Model exchange governance &deprecation planning
- Capstone architecture &roadmap (2–2.5 hours)
- Presentation of end-to-end solution with Agents SDK + RAG
- KPI review &evaluation matrix
- Next steps: AI-102, AZ-204, multi-agent patterns

GOPAS