Week 1: Starting November 10

- **Completed:**
    - Held the initial meeting with the supervisor to introduce the project, clarify expectations, and confirm the weekly reporting and meeting schedule.
    - Completed a literature and landscape review focusing on SQL Agent systems, LangChain SQL workflows, Spider2 SQL benchmark, and modern LLM-based query engines. We reviewed tools from 2024–2025, including multi-agent SQL systems, LangGraph, and open-source alternatives.
    - Explored LangChain's SQL Agent and gained a working understanding of:
        - SQLDatabaseToolkit
        - schema extraction tools
        - SQL safety features
        - differences between create_agent and create_sql_agent
    - Set up and tested the sample SQLite Chinook database:
        - Connected successfully
        - Listed tables
        - Checked schema
        - Executed initial queries
    - Investigated and documented technical challenges:
        - Identified an infinite-loop issue caused by incorrect inputs to sql_db_list_tables
        - Observed how LangChain tools handle schema introspection and safety rules
    - Studied LLM "thought process" traces and applied them to debugging and optimisation.
    - Introduced Human-in-the-Loop (HITL) concepts and discussed how HITL will support accuracy and reliability in SQL generation.
    - Shared and reviewed a high-quality, real-world SQL dataset from Julie's workplace for potential future model evaluation and testing.
    - Defined preliminary team roles:
        - Agent & Retrieval Lead – LangChain wiring, prompts, guardrails
        - Data & SQL Lead – schema design, SQL accuracy
        - UI & DevOps Lead – interface, workflow, deployment
    - Began drafting the project brief, including outline of goals, constraints, innovations, and scope.

- **Planned (Week 2 – 17 to 21 November)**
    - Finalise and submit the Project Brief by 21 November.
    - Set up the GitHub repository and project board (Trello).
    - Decide on the database engine for development (e.g., PostgreSQL, MySQL, SQL Server).
    - Draft initial system architecture diagram, including workflow from UI → LLM → SQL Agent → Database.
    - Continue researching multi-domain SQL agents and adaptability across multiple database types (finance, healthcare, education).

- **Blocking Progress Currently**
    - No blockers at this stage.
    - All Week 1 activities were completed as planned.

- **Reflections**
    - At the start of the week, the team felt slightly overwhelmed by the scope, especially due to the specialised nature of LLM SQL agent technology. However, after meeting with the supervisor and completing the initial research, confidence increased significantly.
    - Reviewing existing commercial and open-source SQL agent systems showed that while many tools exist, most are limited to a single database type or simple queries. This reinforced the value of our chosen innovation direction: multi-dialect, multi-database SQL agents with strong reasoning and guardrails.
    - The team recognised that a key challenge will be creating a system that is not only functional but genuinely distinguishes itself from existing solutions. This will require deeper research, experimentation with prompts, and careful design of retrieval and error-handling modules.
    - Team communication and collaboration started very smoothly, especially with Julie providing a real-world dataset that could support future evaluation work.
- Reference Links
    - LangChain SQL Agent: https://docs.langchain.com/oss/python/langchain/sql-agent
    - Spider 2.0 Benchmark: https://spider2-sql.github.io/
    - Vanna AI (SQL Generative Framework): https://github.com/vanna-ai/vanna/blob/v2/README.md
    - Microsoft SQL Server 2025 innovations: https://learn.microsoft.com/en-us/sql/sql-server/what-s-new-in-sql-server-2025