SQL Statements to create tables and populate them with data:

Table: Students

CREATE TABLE Students (

id INT PRIMARY KEY,

name VARCHAR(50),

age INT,

gender VARCHAR(10),

email VARCHAR(50),

major VARCHAR(50)

);

CREATE TABLE emp

(

emp\_no number(10) NOT NULL,

emp\_name varchar2(50) NOT NULL,

dept\_id number(10),

salary number(6),

CONSTRAINT emp\_pk PRIMARY KEY (emp\_no),

CONSTRAINT dept\_fk

FOREIGN KEY (dept\_id)

REFERENCES dept(dept\_id) );

INSERT INTO Students (id, name, age, gender, email, major)

VALUES (1, 'John Doe', 20, 'Male', 'johndoe@example.com', 'Computer Science');

Table: Courses

CREATE TABLE Courses (

id INT PRIMARY KEY,

name VARCHAR(50),

credit\_hours INT,

instructor VARCHAR(50),

department VARCHAR(50)

);

INSERT INTO Courses (id, name, credit\_hours, instructor, department)

VALUES (1, 'Introduction to Computer Science', 3, 'Dr. Smith', 'Computer Science');

SQL Queries to retrieve data from the database:

Query 1: SELECT \* FROM Students WHERE age > 18;

Output:

id name age gender email major

1 John Doe 20 Male johndoe@example.com Computer Science

Query 2: SELECT \* FROM Courses WHERE department = 'Computer Science';

Output:

id name credit\_hours instructor department

1 Introduction to Computer Science 3 Dr. Smith Computer Science

Query 3: SELECT s.name, c.name FROM Students s JOIN Courses c ON s.major = c.department;

Output:

name name

John Doe Introduction to Computer Science

Security, Integrity, and Ethics:

Security: It is essential to ensure the security of the database by restricting access to authorized personnel only. User accounts and passwords should be created, and access to the database should be granted on a need-to-know basis. All database activity should be monitored and audited regularly to detect any unauthorized access attempts.

Integrity: Data integrity is crucial to ensure the accuracy and consistency of the data stored in the database. Constraints such as primary keys, foreign keys, and check constraints should be enforced to prevent invalid data entry. Regular data backups should also be performed to prevent data loss.

Ethics: It is essential to handle data ethically and in compliance with applicable laws and regulations. The collection, use, and disclosure of personal data should be transparent and based on informed consent. Data should be used only for the purposes for which it was collected and not shared with third parties without the consent of the data subject. Privacy and security should be a top priority in the operation of the database.