INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

_____

2025 y. «16» iyul

Programme	Level 6 Diploma in Data Science		
Unit Number/ Unit Title	UNIT 5 ETHICS, GOVERNANCE AND DATA SECURITY		
Cohort Code:	L06EGDS-U5		
Unit Level	Level 6		
Total GLH	Total qualification time 200/ Total Guided learning hours 90/ Self-guided learning hours 110		
Credits	20 CATS/ 10 ECTS		
Lecturer			
Start Date		**End Date**	

Unit Aims	This unit explores ethical considerations, data governance frameworks, and security best practices for responsible data science in business and research contexts. Students will explore ethical considerations and data governance frameworks essential for responsible data science in both business and research contexts. The unit will cover security best practices to ensure data integrity and privacy, addressing issues such as compliance, risk management, and ethical data usage. By the end of the course, students will be equipped to implement robust data governance strategies and advocate for ethical practices in data science, fostering trust and accountability in their work.
Differentiation Strategies *(e.g. planned activities or support for individual learners according to their needs)*	The total number of students to be in the lesson is approximately 20. This is a multicultural group of students predominantly between the ages of 24 – 45, with numerous ethnic, gender, and creed background. These are UK academic level 5 students; hence it is assumed that they have practical, theoretical, or technological knowledge and understanding of a subject or field of work to find ways forward in broadly defined, complex contexts. These students must be able to generate information, evaluate, synthesise the use information from a variety of

	sources. Various approaches to addressing the various identified students needs will be adopted throughout the lesson. Such will include:- 1. Progressive tasks 2. Digital resources 3. Verbal support 4. Variable outcomes 5. Collaborative learning 6. Ongoing assessment 7. Flexible-pace learning
Equality & Diversity	Variety of teaching techniques will be employed to ensure that the needs of each individual learner are met.
Safeguarding & Prevent	Safeguarding policies and the Prevent duty are strictly observed to ensure the safety, well-being, and inclusivity of all students and staff.
Health & Safety	SIRM H&S policies will be maintained.
Learning Resources	**Teaching and Learning Materials** • O'Neil, C. (2016). Weapons of Math Destruction. Penguin. • Mittelstadt, B., & Floridi, L. (2016). The Ethics of Algorithms: Mapping the Debate. Big Data & Society. • Kitchin, R. (2014). The Data Revolution. SAGE. • UK GDPR and ICO Guidelines.

Learning Outcome	Assessment Criteria
LO1. 1. Examine ethical dilemmas in data science.	Written Report: 1.1 Evaluate data bias and algorithmic fairness 1.2 Assess ethical frameworks (e.g., ACM Code of Ethics).
LO2. 2. Understand data governance frameworks.	Case Study: 2.1 Compare GDPR, HIPAA, and other regulations 2.2 Propose compliant governance policies.
LO3. 3. Implement data protection strategies.	Lab Assignment: 3.1 Use encryption techniques. 3.2 Apply access control and anonymisation methods.
LO4. **5.** Evaluate risks and responsibilities of AI deployment.	Group Debate: 4.1 Critically assess liability in AI decisions. 4.2 Discuss societal impacts of data misuse.

No	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/year/ signature
1.	**Introduction to AI Ethics** Key	**Introduction to AI Ethics** Key principles: Fairness, Accountability, Transparency (FAT)	LO1: Ethical Dilemmas in Data Science	
2.	**Algorithmic Bias & Fairness**	**Algorithmic Bias & Fairness** Case studies: COMPAS, hiring algorithms, facial recognition	LO1: Ethical Dilemmas in Data Science	
3.	**Ethical Frameworks**	**Ethical Frameworks** ACM Code of Ethics, EU Ethics Guidelines for Trustworthy AI	LO1: Ethical Dilemmas in Data Science	
4.	**Privacy vs. Utility Trade-offs**	**Privacy vs. Utility Trade-offs** Data anonymization challenges, re-identification risks	LO1: Ethical Dilemmas in Data Science	
5.	**Human Rights & AI**	**Human Rights & AI** Impact on autonomy, discrimination, and surveillance	LO1: Ethical Dilemmas in Data Science	
6.	**GDPR Deep Dive**	**GDPR Deep Dive** Key provisions, "Right to Explanation," fines	LO2: Data Governance Frameworks	
7.	**HIPAA & Healthcare Data**	**HIPAA & Healthcare Data** PHI protection, de-identification standards	LO2: Data Governance Frameworks	
8.	Half-Term Exam	- Review of LO1 topics - Practice questions and mock assessment	LO1 LO2	

		- **Half-term assessment** based on LO1 (theory)		
9.	**CCPA & Global Privacy Laws**	**CCPA & Global Privacy Laws** Comparison with Brazil's LGPD, India's DPDPA	LO2: Data Governance Frameworks	
10.	**Industry-Specific Regulations**	**Industry-Specific Regulations** FINRA (finance), FERPA (education)	LO2: Data Governance Frameworks	
11.	**Designing Governance Policies**	**Designing Governance Policies** Roles of DPOs (Data Protection Officers), audit trails	LO2: Data Governance Frameworks	
12.	**Encryption Techniques**	**Encryption Techniques** AES, RSA, TLS, homomorphic encryption (conceptual)	LO3: Data Protection Strategies	
13.	**Access Control Models**	**Access Control Models** RBAC (Role-Based Access Control), ABAC (Attribute-Based)	LO3: Data Protection Strategies	
14.	Final Exam Preparation & Review	- Comprehensive review of all learning outcomes - Practice questions and revision of key topics		
15.	Final Exam	- **Final-term assessment** covering all learning outcomes (theory and practical elements)		
16.	Feedback & Reflection	- Review of final exam - Individual feedback on performance - Reflective discussion on key learning points		
17.	**Anonymization Methods**	**Anonymization Methods** k-Anonymity, l-Diversity, differential privacy	LO3: Data Protection Strategies	
18.	**Data Masking & Tokenization**	**Data Masking & Tokenization** Use cases in payment processing, healthcare	LO3: Data Protection Strategies	

19.	**Secure Data Lifecycle**	**Secure Data Lifecycle** From collection to deletion (NIST guidelines)	LO3: Data Protection Strategies	
20.	**Liability in AI Systems**	**Liability in AI Systems** Case study: Tesla Autopilot accidents, medical AI errors	LO4: AI Risks & Societal Impact	
21.	**AI & Employment Disruption**	**AI & Employment Disruption** Automation trends, reskilling strategies	LO4: AI Risks & Societal Impact	
22.	**Misinformation & Deepfakes**	**Misinformation & Deepfakes** Detection tools, regulatory responses	LO4: AI Risks & Societal Impact	
23.	Half-Term Exam	**Project** Design a governance framework for a real-world AI use case		
24.	**Environmental Impact of AI**	**Environmental Impact of AI** Carbon footprint of LLMs, sustainable AI	LO4: AI Risks & Societal Impact	
25.	**Global AI Governance**	**Global AI Governance** UN initiatives, OECD AI Principles	LO4: AI Risks & Societal Impact	
26.	**Ethical Impact Assessment (EIA)**	**Ethical Impact Assessment (EIA)** Templates, risk matrices, stakeholder engagement	LO5: Capstone & Practical Applications	
27.	**Bias Mitigation Lab**	**Bias Mitigation Lab** Hands-on with IBM AIF360 or Fairlearn	LO5: Capstone & Practical Applications	
28.	**Data Breach Simulation** and **Debate: "Should AI Have Legal Personhood?"**	**Data Breach Simulation** Incident response planning, GDPR breach reporting **Debate: "Should AI Have Legal Personhood?"** Student-led discussion on accountability	LO5: Capstone & Practical Applications	
29.	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30.	Final Exam		LO1, LO2, LO3, LO4	