Programme Regulations: 2023/24

Programme Titles:
Degree of Master of Computing with Honours in Computer Science (Cyber Security)– UCAS Code: I198
Degree of Master of Computing with Honours in Computer Science with Industrial Placement (Cyber Security) – UCAS Code: I197

Notes
(i)   *These programme regulations should be read in conjunction with the University's Taught Programme Regulations.*
(ii)   *All optional modules are offered subject to the constraints of the timetable and to any restrictions on the number of students who may be taught on a particular module. Not all modules may be offered in all years.*
(iii)   *Unless otherwise stated under 'Type', modules are not core.*
(iv)   *A compulsory module is a module which a student is required to study.*
(v)   *A core module is a module which a student must pass, and in which a fail mark may neither be carried nor compensated; such modules are designated by the board of studies as essential for progression to a further stage of the programme or for study in a further module. Unless otherwise stated, modules are not core.*
(vi)   *All modules are delivered in Linear mode unless stated otherwise as Block, eLearning or distance learning.*
(vii)   *Programme transfers for Tier 4 students may be restricted by current Tier 4 rules. Please refer to the Visa Team for advice.*

1.   Stage 1

(a)   All candidates shall take the following compulsory modules:

Code	Descriptive title	Total Credits	Credits Sem 1	Credits Sem 2	Level	Type
CSC1031	Fundamentals of Computing	20	10	10	4	
CSC1032	Computer Systems Design and Architectures	20	10	10	4	
CSC1033	Foundations of Data Science	20	10	10	4	
CSC1034	Programming Portfolio 1	30	30		4	
CSC1035	Programming Portfolio 2	30		30	4	

2.   Stage 2

(a)   All candidates shall take the following compulsory modules:

Code	Descriptive title	Total Credits	Credits Sem 1	Credits Sem 2	Level	Type
CSC2031	Security and Programming Paradigms	20	20		5	
CSC2032	Algorithm Design and Analysis	10	10		5	
CSC2033	Software Engineering Team Project	30		30	5	Block
CSC2034	Introducing Contemporary Topics in Computing	30		30	5	Block
CSC2035	Software Systems Design and Implementation	30	30		5	

3.   Intercalating Year – I194 only

Upon completion of Stage 2 and before entering Stage 3, all candidates shall spend the equivalent of one academic year in a placement approved by the Placement Coordinator. If a candidate is not successful in securing an approved placement, or fails the assessment of the placement year, then the candidate will be required to transfer to Stage 3 of I192.

Code	Descriptive title	Total Credits	Credits Sem 1	Credits Sem 2	Level	Type
ICM0043	Intercalating Module for Computing Science Programmes	120	60	60	6	

4. Stage 3

(a) All candidates shall take the following compulsory modules:

Code	Descriptive title	Total Credits	Credits Sem 1	Credits Sem 2	Level	Type
CSC3094	Major Project and Dissertation in Computer Science	60		60	6	
CSC3631	Cryptography	10	10		6	
CSC3632	System and Network Security	20	20		6	

(b) All candidates shall select a further 30 credits of optional modules from the table below. Candidates may not select more than one 10 credit module.

Code	Descriptive title	Total Credits	Credits Sem 1	Credits Sem 2	Level	Type
CSC3121	Distributed Systems	10	10		6	
CSC3231	Graphics for Games	10	10		6	
CSC3232	Gaming Technologies and Simulations	20	20		6	
CSC3334	Science of Computing	20	20		6	
CSC3431	Introduction to BioDesign and Natural Computing	20	20		6	
CSC3432	Biomedical Data Analytics and AI	20	20		6	
CSC3634	Fault Tolerant and Cyber-Physical Systems	20	20		6	
CSC3731	Human Computer Interaction: Interaction Design	20	20		6	
CSC3831	Predictive Analytics, Computer Vision & AI	20	20		6	
CSC3833	Data Visualization and Visual Analytics	10	10		6	
NCL3007	Career Development for Final Year Students	20	10	10	6	

(c) Candidates may take modules from other Schools to a value of 20 credits, subject to the approval of the Degree Programme Director. NCL3007 is treated as 20 credits from another School and is subject to the approval of the Degree Programme Director.

5. Stage 4

(a) All candidates shall take the following compulsory modules:

Code	Descriptive title	Total Credits	Credits Sem 1	Credits Sem 2	Level	Type
CSC8103	Distributed Algorithms	10	10		7	Block
CSC8106	System Evaluation	10	10		7	Block
CSC8202	Information Security and Cryptography	10	10		7	Block
CSC8204	Secure Software Development	10	10		7	Block
CSC8208	Research Methods and Group Project in Security and Resilience	20		20	7	Block
CSC8216	Risk & Trust Management	10	10		7	Block
CSC8498	Project and Dissertation for MComp	30		30	7	

(b) All candidates shall choose one of the following optional modules:

Code	Descriptive title	Total Credits	Credits Sem 1	Credits Sem 2	Level	Type
CSC8110	Cloud Computing	10	10		7	Block
CSC8111	Machine Learning	10	10		7	Block

(c)   All candidates shall choose one of the following optional modules:

Code	Descriptive title	Total Credits	Credits Sem 1	Credits Sem 2	Level	Type
CSC8101	Engineering for AI	10		10	7	Block
CSC8207	Security of Complex Systems	10		10	7	Block

6.   Assessment methods
Details of the assessment pattern for each module are explained in the module outline.

7.   Progression and transfer to other programmes
Candidates wishing to progress to Stage 3 must pass Stage 2 with a stage average mark of at least 50%. Candidates who fail to satisfy this criterion are normally required to transfer to the degree of Bachelor of Science with Honours in Computer Science (Security and Resilience).

For students entering in 2018/19 onwards, candidates wishing to progress to Stage 3 must pass Stage 2 with a stage average mark of at least 60%. Candidates who fail to satisfy this criterion are normally required to transfer to the degree of Bachelor of Science with Honours in Computer Science (Security and Resilience).

Candidates wishing to progress to Stage 4 are normally required to pass all Stage 3 modules with a stage average mark of at least 60%. Candidates who fail to satisfy this criterion shall be considered for the award of Bachelor of Science with Honours in Computer Science (Security and Resilience).

8.   Degree title
Candidates who fail to satisfy the requirements for the award of Master of Computing with Honours in Computer Science (Security and Resilience) shall be considered for the award of Bachelor of Science with Honours in Computer Science (Security and Resilience).

Candidates who fail to satisfy the requirements for the award of Master of Computing with Honours in Computer Science with Industrial Placement (Security and Resilience) shall be considered for the award of Bachelor of Science with Honours in Computer Science with Industrial Placement (Security and Resilience).

9.   Degree classification
Candidates will be assessed for degree classification on the basis of all the modules taken at Stages 2, 3 and 4 with the weighting of the stages being 1:2:2 for Stage 2, Stage 3 and Stage 4 respectively.