MODULE SPECIFICATION

Part 1: Information			
Module Title	Internet of Things (IoT)		
Module Code	UFCFBR-30-3	Level	Level 6
For implementation from	2019-20		
UWE Credit Rating	30	ECTS Credit Rating	15
Faculty	Faculty of Environment & Technology	Field	Computer Science and Creative Technologies
Department	FET Dept of Computer Sci & Creative Tech		
Module type:	Standard		
Pre-requisites	None		
Excluded Combinations	None		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description

Overview: The Internet of Things (IoT), is the connecting and internetworking of multiple devices over the internet, allowing them to communicate with us, applications, and each other.

Educational Aims: This module aims to provide learners with an in-depth appreciation of the Internet of Things (IoT) and the tools to design and develop their own multi-device IoT Solution to meet a project requirement.

In completion of this module learners should be able to:
Plan, develop and test a secure multi-client IoT solution to meet a defined scenario using suitable IoT enabled hardware and software. Software languages could include Windows IOT Core, Python.
Node/Node Red, C. Suitable IoT hardware devices:
Raspberry Pi
Arduino
BeagleBoard
Intel Edison
Google Coral
Evaluate different M2M protocols (eg technology, range, costs, bandwidth, regulation, limitations)
Use a variety of sensors to monitor, record data and trigger actions accordingly
Province clear and meaningful user access to sensors/data via a web accessible interface or

dashboard hosted on a suitable web/cloud/IoT hosting platform.
Identify key legislation impacting the publication of IoT Solutions, eg Data Governance (IPO, GDPR, Data Protection), privacy policies, use of data etc.

Outline Syllabus: Delivery will cover modern system architecture, key technologies, and legal, social and ethical/moral implications to implementing these technologies.

System architecture (e.g. centralised and decentralised)
Machine-to-Machine (M2M) Communication (e.g. Wireless technologies, Messaging/communication protocols)

Hardware and software platforms for IoT
Legal, social, ethical, and moral implications of IoT
Effective cyber security in relation to IoT
Students will be able to cultivate independent technical judgement in the use of techniques and tools associated with IoT devices and M2M communication protocols. As well as being able to develop the ability to think conceptually and translate concepts into reality, learners will go beyond programming web applications, and develop skills in security, penetration testing and user experience.

Teaching and Learning Methods: Introductory lectures are supported by seminars, case studies, visits and practical workshops. In addition this module will be supported by interactive forums and learning tools. Students must have access to a suitable publicly accessible hosting platform and database server to be able to complete this module.

300 hours study time of which 108 hours will represent scheduled learning. Scheduled learning includes lectures, seminars, tutorials, demonstration, practical classes and workshops; external visits; supervised time in studio/workshop.

Part 3: Assessment

This module is assessed by a combination of techniques: an examination and a practical portfolio.

Exam (includes the following):
Fundamentals of IoT technology (e.g. Hardware, software, sensors, frameworks)
Evaluate/compare different M2M protocols
Key legislation impacting the publication of IoT Solutions, e.g. Data Governance (IPO, GDPR, Data Protection), privacy policies, use of data etc.

Practical Portfolio (includes the following):
Evidence of planning and design of a IoT solution to support an agreed scenario
Implementation of an IoT solution to support a scenario consisting of a minimum of two interconnected devices and a selection of suitable sensors.
Deploying and test a completed IoT solution
Documenting complete IoT solution

Opportunities for formative assessment exist for the assessment strategy used. Verbal feedback is given and all students will engage with personalised tutorials setting SMART targets as part of the programme design.

First Sit Components	Final Assessment	Element weighting	Description
Practical Skills Assessment - Component B	✓	70 %	Practical Skills Assessment - Design, build, and test an IoT solution
Examination - Component A		30 %	Exam (1.5 Hours)

Resit Components	Final Assessment	Element weighting	Description
Practical Skills Assessment - Component B	✓	70 %	Practical Skills Assessment - Design, build, and test an IoT solution
Examination - Component A		30 %	Exam (1.5 Hours)

Part 4: Teaching and Learning Methods

Learning Outcomes

On successful completion of this module students will achieve the following learning outcomes:

Module Learning Outcomes	Reference
Explain common security risks present when building and publishing web driven IoT solutions and best practice authentication (e.g. injection protection, code injection/data validation, protection from brute force attacks, encryption techniques, end to end encryption).	MO1
Evaluate key IoT hardware and software solutions	MO2
Evaluate different M2M protocols	MO3
Plan, develop and test a secure multi-client IoT solution to meet a defined scenario using suitable IoT enabled hardware and software.	MO4
Use a variety of sensors to monitor, record data and trigger actions to empower a complete IoT solution	MO5
Understand key legislation impacting the publication of IoT Solutions	MO6

Contact Hours

Independent Study Hours:	
Independent study/self-guided study	192
Total Independent Study Hours:	192
Scheduled Learning and Teaching Hours:	
Face-to-face learning	108
Total Scheduled Learning and Teaching Hours:	108
Hours to be allocated	300
Allocated Hours	300

Reading List

The reading list for this module can be accessed via the following link:

https://uwe.rl.talis.com/index.html

Part 5: Contributes Towards
This module contributes towards the following programmes of study: