This Version is No Longer Current
The latest version of this module is available here

MODULE DESCRIPTOR

Module Title

Computer Ethics and Law

Reference	CM3100	Version	2
Created	April 2017	SCQF Level	SCQF 9
Approved	July 2016	SCQF Points	15
Amended	August 2017	ECTS Points	7.5

Aims of Module

To provide students with the ability to independently and as a team member identify, analyse, discuss and report key issues of ethics and law that relate to computer security for both individuals and society. Students will also be provided with an opportunity to explore and understand the importance of the roles users play in cyber security. This includes positive and negative aspects, human error versus premeditated actions and behaviours.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1	Identify important ethical and legal issues that impact on professional behaviour linked to computer security.
2	Research and analyse material and real-world situations that relate to ethical and legal issues linked to human aspects of security.
3	Systematically debate, discuss and report the outcomes of investigations.
4	Provide advice and recommendations about how to tackle ethical and legal issues linked to security.
5	Apply industry standards and guides of best practice to situations involving information security.

Indicative Module Content

Legal and ethical frameworks; codes of conduct and professional societies. Modern security concerns and cyber issues; privacy, sharing; hacking. Interpreting laws and approaches to ethical analysis; case studies. Human in the loop; human errors and security vulnerabilities and how to counter them. Analytical skills and systematic analysis; debating, reporting, writing and oral skills. Cyber terrorism; cyber defence; professional roles. Standards and Best Practice Guides: ISO 27001, ISO 27014, ISO 27036.

Module Delivery

This module is delivered through lectures, tutorials and assessed practical work with formative feedback.

Module Ref:	CM3100 v2

Indicative Student Workload	Full Time	Part Time
Contact Hours	36	N/A
Non-Contact Hours	114	N/A
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	N/A
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	100%	Outcomes Assessed:	1, 2, 3, 4, 5
Description:	Coursework.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of C1. An overall minimum grade D is required to pass the module.

Module Grade	Minimum Requirements to achieve Module Grade:
A	The student needs to achieve an A in Component 1
B	The student needs to achieve a B in Component 1
C	The student needs to achieve a C in Component 1
D	The student needs to achieve a D in Component 1
E	The student needs to achieve an E in Component 1
F	The student needs to achieve an F in Component 1
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	CM2102 Real World Project & Professional Skills, or equivalent.
Corequisites for module	None.
Precluded Modules	None.

INDICATIVE BIBLIOGRAPHY

1	MANJIKIAN, M. 2018. Cybersecurity Ethics: An Introduction. Taylor & Francis
2	TAVANI, H. T., 2013. Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing. 4th ed. Wiley.
3	FRIEDMAN, B., HENDRY, D. G. 2019. Value Sensitive Design: Shaping Technology with Moral Imagination. MIT Press