Unit Title	Cyber Ethics, Regulation and Compliance (blended)
FHEQ Level	Level 6
Unit Code	CYS20303
Credit Value	15
Unit Type	Subject

Learning Hours			
Staff – Student Contact Hours		**Independent Study Hours**	
Classes	30	Independent study	90
Supervised access to Ravensbourne resources	0	Preparation for assessment	30
Total		150	

Unit Description

This unit will introduce students to the regulatory framework within organisations and countries, compliance with these rules and ethical issues surrounding the cyber world.

Confidentiality is one of the key elements in any organisation and maintaining it can be challenging where data is stored in the cloud or hackers may have access to it through the internet

Cyberworld is full of hackers who would try to exploit every vulnerability to gain unauthorised access. Same as someone trying to break into a house or in an organisation, breaking rules, regulations and ethical barriers. When deploying any cyber solutions, access to personal data and administrative rights to machines may bring a new challenge.

Bring Your Own Device (BYOD) and various models of cloud computing bring a new challenge to data security. Storage of data out of the country's jurisdiction may compromise data and very little could be done legally to prevent it.

The unit will also cover Legal aspects regarding collection, storage and processing of data (Data Protection Act, Computer Misuse Act). Ethical considerations such as the types of data collected will also be evaluated.

It is also important to be aware of types of data collected by Industry 4.0 systems. The unit will also explore the moral hazard where hackers try to gain access to personal organisational data with the help of insiders.

The Five Principles underpin the Mindsets and Skillsets Manifesto and are the foundation upon which all course curriculum frameworks and unit specifications are based. The relevant Principles as stated below have been mapped against the Learning Outcomes

relevant to each course unit and at each level (see Programme Specifications for full description of the Five Principles):

1. Cultivate / Where the individual thrives.
2. Collaborate / Where disciplines evolve.
3. Integrate / Where education engages industry.
4. Advocate / Where purpose meets practice.
5. Originate / creativity meets technology.

Unit Indicative Content

Cyber Ethics, Regulations and Compliance

Industry-wide Knowledge

- Confidentiality
- Moral Hazard
- Incident Response
- Roles and Responsibilities
- Law & Regulation
- Application of Law to Cyber Space
- Jurisdiction issues in Cyber World
- Privacy Laws and Data Protection
- Online Contracts
- Duty of Care
- Intellectual property
- Ethics
- Human behaviour in security
- Privacy and Online rights

CyBOK knowledge areas

- Human, Organisational and Regulatory Aspects
- Law & Regulation
- Human Factors
- Privacy & Online Rights

Unit Aims

- To be able to evaluate potential ethical and moral issues surrounding digital systems.

- To be able to demonstrate an understanding of legal implications of data storage in cloud-based networks in conjunction with jurisdiction and data protection laws
- To be bale to appraise risk management techniques and human factors involved in data security
- To be able to demonstrate an understanding of Criminal and Civil Law related to Digital Systems

Unit Learning Outcomes *(to be selected from the Mini Manual)*
LO 1 Research/Inspiration Select and evaluate information gathering techniques using a wide range of sources, providing visual, contextual and industry case-study research as appropriate. Related Principle: **ORIGINATE**
LO 2 Concept/Ideation Critically appraise and evaluate appropriate research materials to generate workable concepts or strategic project themes that inform and underpin project development. Related Principle: ORIGINATE
LO 6 Critical and creative mindsets Evaluate a range of critical approaches in order to form an independent position Related Principle: ORIGINATE

Learning and Teaching Methods

This unit will be delivered using a combination of:

- Lectures / Seminars
- Online activities
- Self-directed independent study
- Peer learning, group discussion, guest speakers

Assessment methods and tasks	
Assessment tasks	**Weighting (%)** *(one grade or multi-grade unit)*
A portfolio of practical outcomes which might include tests, experiments, research and development material and research log	50%
Online Test	50%

Indicative Assessment Criteria

With the help of various case studies and examples

- Critically evaluate potential ethical and moral issues surrounding digital systems. (LO6)
- Explain what is Moral Hazard and how it may have an impact on confidentiality (LO1)
- Create an incident response plan (LO2)
- Critically evaluate the implications that may be caused by Jurisdiction issues in Cyber World (LO6)
- Evaluate the implications of law enforcement in cyber world, what could be the potential issues in terms of Privacy Laws and Data Protection (LO1, LO6)
- Analyze the implications of online contracts, intellectual property, privacy and online behaviours (LO2, LO6)

Essential Reading list

The Cyber Security Body of Knowledge. (2019). 1st ed. The National Cyber Security Centre.

Government Digital Service. “Data Protection.” GOV.UK, GOV.UK, 16 Sept. 2015, www.gov.uk/data-protection.

Recommended Reading List

“NCSC Code of Conduct.” Ncsc.gov.uk, www.ncsc.gov.uk/information/ncsc-code-conduct.

“Guide to Data Protection.” ICO, ico.org.uk/for-organisations/guide-to-data-protection/.

Participation, Expert. “Official Secrets Act 1989.” Legislation.gov.uk, Statute Law Database, 11 May 1989, www.legislation.gov.uk/ukpga/1989/6.

Participation, Expert. “Computer Misuse Act 1990.” Legislation.gov.uk, Statute Law Database, 29 June 1990, www.legislation.gov.uk/ukpga/1990/18/contents.

Participation, Expert. “The Privacy and Electronic Communications (EC Directive) Regulations 2003.” Legislation.gov.uk, Statute Law Database, www.legislation.gov.uk/uksi/2003/2426.

Further reading and resources may be identified in your Project Brief.