Programme Specification

A Programme Specification provides a concise summary of the main features of a programme and its intended learning outcomes. It is intended to be used by prospective students, current students, academic staff and potential employers.

Programme Title:	
MSci (Hons) Cyber Security	
Programme (AOS) Code(s):	**MB1CYB1**
UCAS Code:	**MCYB**
Name of Final Award:	**Master in Science, MSci**
Level of Qualification:	**Level 7**
Regime of Delivery:	**Attendance**
Mode(s) of Delivery:	**Full Time**
Typical Length of Study (Years):	**4 Years**
Professional Body Recognition / Accreditation (including specific requirements where applicable):	**N/A**

Brief Description of the Programme

The security concept is a rapidly growing element of the industry sector due to the significant increment information, privacy and system breaching and attacks. There are many skills required of adept and effective security specialists, who may be responsible for sensitive activities, information and projects.

Cyber-attacks comprise the main security issues facing organisations in the information age. Today, all organisations operate with a potential information security risk and will need to implement strategies to protect their information technology (IT) systems and data. Although society has become increasingly reliant upon IT and cloud based services, cyber security skills and capability are not currently increasing at a comparable rate.

This programme is designed to provide prospective and practicing cyber security specialists with a range of skills and develop knowledge in order to be able to operate with confidence within the cyber security sector. It aims to meet the needs of students who want to improve their technical and managerial CS skills. The course will provide a combination of studies of subject areas which will provide a solid educational basis for the technical and management cyber security solutions.

The programme is to offer students with an academically rigorous, relevant and industry-related program which will allow them to provide business-orientated security experience based upon knowledge, best practice and regulatory guidance.

As one of leading industrial countries, the UK has considered cyber security as one of the most important concepts for providing safe and reliable products and service. Therefore, the UK prioritises Cyber Security and aim to become the world leader in the cyber security sector.

Qualified cyber security professionals are currently in high demand by business, government and law enforcement agencies across the globe. Graduating students from the course will have gained the fundamental skills and knowledge necessary to quickly adopt the emerging technologies and

concepts in this fast changing field, alongside the professional and business skills, techniques and ways of thinking needed to be able to align technical security requirements with business needs.

The MSci Cyber Security program has been developed to provide a specific opportunity for students to enter an educational programme in an increasingly vital subject area. The course is designed for those wishing to develop their careers as cyber security professionals, to develop new skill sets that may enable them to consider alternative employment roles in IT services, or to develop or apply cyber security solutions in a strategic, technical, business, consultancy or management context.

The course is focused to cover both technical and management aspects needed in the cyber security sector. The balance between the two perspectives will give the students the ability to act as security specialists in both areas, and to increase and enhance their employability prospects.

Distinguishing Features

- The MSci (Hons) Cyber Security course reflects current sector currency, employer and industry requirements
- This program has been structured to include highly demanded technical and management security technologies, trends and polices to prepare learners/students for work in this fast-moving sector

This will equip students with the skills you'll need to get hired in one of the fastest-growing industries.

Professional Development

A major benefit of Integrated Master's degree courses is the final year project which will help you to develop advanced technical and professional skills that are required for research or other practically-based careers.

A Masters at no extra cost

All four years of an Integrated Master's degree are eligible for undergraduate student finance including tuition fee loans and maintenance loans and grants.

Advanced, Expert Skills

An Integrated Master's degree allows you to stand out from the crowd in competitive jobs market. Employers are increasingly looking for employees with the advanced technical skills and expert understanding provided by an Integrated Master's degree course.

Top class learning experience

We encourage problem-based learning through case studies and classroom-based exercises throughout our modules.
We have first class learning facilitates to equip you with the skills that match requirements of the top employers in the industry. Throughout the year you'll have access to both our specialist computing suite in the Gateway building at our High Wycombe campus and our Cyber Resilience Centre.

Experienced Lectures

Our lecturers have extensive industry and academic experience. They'll help you mix theory with practice, informing your teaching with their knowledge. We attract many guest speakers from industry, who share their business acumen, inform on current practices, career opportunities, and help prepare you for working life as a cyber security professional.

More placements, more choices
Bucks is a Placements Plus university. So, whatever degree you do, you can be sure there'll be plenty of industry-relevant opportunities on offer, to help you get into your chosen field.
We'll also prepare you for work beforehand, with special skills for work training, further boosting your CV, and building skills employers will value. In recognition of the value we place on these skills we have incorporated this experience into your study time.
Placements Plus is all about helping you get some valuable experience under your belt while you're a student. To increase your choices later, and help you get the graduate-level job you want.

COURSE DETAILS
Our MSci (Hons) Cyber Security programme combines three years of undergraduate study with an additional fourth year at postgraduate level, in a single course.

The Integrated Master's degree is identical to the equivalent undergraduate course, but provides you with the opportunity to explore your interest in greater detail by offering a fourth year of study, enabling you to graduate with a Masters degree.

This programme focuses on providing students insight into the context of the needs of real organisations by exploring their current and future operating environments.

During the course, you'll also learn to use a wide range of cyber security related tools and techniques, alongside specialist technical skills in computer programming, software engineering, cloud and database development.

You'll learn modern technical system tools like Network and Software security, Artificial Inelegant systems security, cloud computing system security, and mobile systems security, as well as developing management skills in business continuity and disaster recovery, cyber security assurance and risk management, in addition to research techniques.
All modules have been designed with input from key industry governing bodies and experts such as the Communications-Electronics Security Group (CESG), a group within the UK Government Communications Headquarters (GCHQ), as well as Institute of Information Security Professionals (IISP) Information Security Skills Framework.
As you progress, you'll gain a solid understanding of how to protect organisations, networks, IT systems and individuals against cyber-attacks and cyber threats. You'll be given the opportunity to become more effective and creative when solving cyber security problems, as well as analysing scenarios with a view to being able to advise individuals.

If you do not achieve the necessary standard of performance to continue onto the fourth year and complete the Integrated Masters, you can still graduate after three years with a Bachelor degree qualification.

Course option pathways

Programme Aims

1	Develop a high level of theoretical and practical knowledge in cyber security
2	Provide students with a deep understanding of technical decisions involving commercial cyber security provision and the development of an awareness of various essential technologies related to this provision.
3	Enable students to become capable in a range of cyber security skills, tools and solutions
4	Develop skills in independent learning, decision making and research in cyber security
5	Improve leadership and management skills to enable the effective management of security systems and business positions in the cyber security sector.

Programme Learning Outcomes

The Bucks Graduate Attributes focus on the development of innovative leaders in professional and creative capacities, who are equipped to operate in the 21st Century labour market and make a positive impact as global citizens. The attributes are developed through the programme.

ID	Learning Outcome
On successful completion of the programme, the student will be able to:	
Graduate Attribute: Knowledge and its application (K)	
K1	Appreciate the core disciplines of cyber security including: information security, software security, programming, database security and network security.
K2	Identify the practical security requirements for both computer and cloud-based systems including the recognition and analysis of criteria and models leading to specifications used in the solution of specific cyber security problems.
K3	Explain the mathematical principles that underpin computer-based systems.
K4	Acknowledge the key activities prevalent in the software lifecycle, alongside their outputs and dependencies between stages, alongside the ethical, professional and legal standards required.
K5	Recognise the business, industrial and commercial context in which cyber security is deployed, with particular regard to its usability.

K6	Critically evaluate global contemporary issues relating to Cyber Security techniques, management, and solutions
K7	Appreciate the core disciplines of cyber security including: information security, software security, programming, database security and network security.
K8	Demonstrate critical consideration of key concepts, issues and theories related to the development, management and marketing of security businesses
K9	Consolidate and synthesise a coherent body of knowledge in order to execute a sustained piece of independent work using appropriate media
Graduate Attribute: Creativity (C)	
C1	Evaluate and deploy approaches to modelling in order to design computer-based information systems, with particular regard to the cyber security paradigm.
C2	Solve problems in a logical and analytical manner.
C3	Plan, manage, undertake and report on a significant project.
C4	Make informed decisions and produce innovative plans, approaches and solutions to software issues within a quality assurance and testing framework.
C5	Appreciate the role of critical evaluation and testing in ensuring that computer-based information systems are secure and meet the criteria for their defined use and future developments.
C6	Critically evaluate technical, business and human features of cyber security.
C7	Appraise new and emerging computer related technologies with particular regard to Cloud Computing and Security Systems.
C8	Appreciate the unique challenges associated with the development and deployment of mobile and Web-based systems.
C9	Critically evaluate arguments, assumptions, abstract concepts and data to make creative informed judgments
C10	Wisely apply theory to practice in the strategic management and technical solutions of security systems within organisations
C11	Judiciously select effective solutions in the development of appropriate security systems
Graduate Attribute: Social and ethical awareness and responsibility (S)	
S1	Analyse, design, develop and maintain reliable secure software and network systems, with particular regard to Information Systems encapsulated in a Quality Assurance Framework.
S2	Employ analytical techniques and design tools in the development of secure software and network system artefacts.
S3	Apply sound programming principles to the construction and maintenance of secure software deployed on multiple platforms, using appropriate programming paradigms and languages.
S4	Evaluate a system in terms of quality and associated trade-offs.
S5	Recognise the risks or safety aspects associated with various computer-based systems.
S6	Specify, design, implement and test computer-based Information Systems.
S7	Evaluate and deploy approaches to modelling in order to design computer-based information systems, with particular regard to the cyber security paradigm.

S8	Critically evaluate arguments, assumptions, abstract concepts and data to provide best technical/managerial consultation, decisions and/or solutions.
S9	Critically consider how ethical and cultural values - including the student's own - have an impact on responses to and rival interpretations of security and related subjects
S10	Synthesise and evaluate information from a wide variety of sources relating to cyber security and business issues
Graduate Attribute: Leadership and self-development (L)	
L1	Employ information-retrieval skills (including browsers, search engines and catalogues).
L2	Demonstrate numeracy and literacy in both understanding and presenting cases involving a quantitative and qualitative dimension.
L3	Work as a member of a development team, recognising the different roles within a team and different ways of organising teams.
L4	Manage one's own learning and development including time management and organisation skills.
L5	Appreciate the need for continuing professional development in recognition of the need for lifelong learning.
L6	Develop theoretical and practical strategic management and technical solutions of security systems within organisations
L7	Critically evaluate theories, principles, concepts and factual information in the development of solutions to cyber security problems
L8	Demonstrate confident leadership in building and developing efficient security systems in response to cyber security problems

Programme Structure

Programmes are structured in stages. The number of stages will vary depending on the mode (e.g. full-time, part-time), duration and location of study which will be detailed in the Programme Handbook.

Modules are set at a specific academic level and listed as either core (compulsory) or optional. The level indicates the relative academic difficulty which will increase through the programme. Passing modules will reward you with academic credit. The amount of credits will depend on the complexity of the module and the level of effort required, which is measured in 'notional learning hours'.

Our Academic Advice webpages provide more information on the structure of taught awards offered by the University.

Please note: Not all option modules will necessarily be offered in any one year. Other option modules may also be introduced at a later stage enabling the programme to respond to sector developments.

Level Four

Code	Module Title	Credit	Core / Option	Compensable (Normally Yes)
CO403	Secure Systems	15	Core	Yes
CO404	Cyber Threat and Risk Management	15	Core	Yes
CO450	Computer Architectures	15	Core	Yes
CO451	Networking	15	Core	Yes
CO452	Programming Concepts	15	Core	Yes
CO453	Application Programming	15	Core	Yes
CO454	Digital Technologies & Professional Practice	15	Core	Yes
CO456	Web Development	15	Core	Yes

Level Five

Code	Module Title	Credit	Core / Option	Compensable (Normally Yes)
CO506	Information Security	15	Core	Yes
CO507	Cyber Security Management	15	Core	Yes
CO508	Mobile Systems Security	15	Core	Yes
CO551	Open Source Systems	15	Core	Yes
CO556	Network Systems	15	Core	Yes
CO557	Software Engineering	15	Core	Yes
CO558	Database Design	15	Core	Yes
CO559	Intro to Intelligent Systems (Team Project)	15	Core	Yes

Level Six

Code	Module Title	Credit	Core / Option	Compensable (Normally Yes)
CO651	Quality Assurance & Testing	15	Core	Yes
CO652	Knowledge-Based Systems in A.I	15	Core	Yes
CO653	Learning Machines and Intelligent Agents	15	Core	Yes
CO654	Cloud Computing	15	Core	Yes
CO655	Network Security	15	Core	Yes
CO666	Advanced Mobile Systems	15	Core	Yes
CO669	Security Auditing and Response	15	Core	Yes
CO670	Secure Business Management	15	Core	Yes

Level Seven

Code	Module Title	Credit	Core / Option	Compensable (Normally Yes)
CO703	Cyber Security in Network Systems	30	Core	Yes
CO707	Project	60	Core	No
Students will also study 30 credits from the following options:				
CO701	Risk Management and Cyber Security Assurance	15	Option	Yes
CO702	Mobile and Information Systems Security Management	15	Option	Yes
CO704	Cloud Security	15	Option	Yes
CO705	Business Continuity and Disaster Recovery	15	Option	Yes

Learning and Teaching Activities

Please see the Academic Advice pages for a description of learning and teaching activities that are recognised by the University. Detailed information on this specific programme is outlined below:

The MSci Cyber Security programme provides varied learning and assessment activities. Modules on this programme will be taught in line with best practice across the university and in the sector. A variety of approaches, and good use of the latest technology, will be blended together to engage students in learning in class and beyond, and to encourage full student participation. The course team will strive to ensure that all modules embrace current industrial practice wherever possible. A range of teaching methods will be used including:

Lectures
This is the most formal teaching strategy employed in teaching the modules. It is generally used to deliver a body of theoretical information to a group of students and is most effective when followed up by a seminar, practical or tutorial session to consolidate learning.

The lecture format may be supported by written hand-outs, slides, web or library references which serve to reinforce and expand the audio-visual information presented. In addition, staff will make appropriate use of the VLE (Blackboard) facilities or any other appropriate facility. This should enable lecturers to enhance the traditional communication and learning mediums, as well as making material available to students at home and university.

Tutorials / Practical Sessions
Often in smaller groups, tutorials are guided learning sessions, which can either support a formal lecture by students working through tutorial sheets with the help of a lecturer or by students working through practical exercises in say a computing room.

Seminars
These can vary from large group seminars, which provide an opportunity for the student-led formal debate of particular topic areas, to 'impromptu' discussion sessions with smaller groups, which may for example follow the showing of a video.

Other techniques such as industrial visits, guest lectures and computer aided learning tools such as the university's VLE will be used where appropriate. This variety of techniques is aimed at stimulating student learning. The teaching and learning strategies for individual modules are detailed in the relevant module pro-forma.

Additional Course Costs

There are costs associated with all studies, additional to the tuition fee, which require consideration, when planning and budgeting for expenditure. Costs are indicative and for the total length of the course shown unless otherwise stated and will increase with inflation; depending on the programme they may include equipment, printing, project materials, study trips, placement activities, DBS and/or other security checks.

Books and other Texts:
All core texts will be in the library for students to borrow for free, and wherever possible texts on reading lists will also be purchases in the library. Students may be required to purchase texts and journals to support their study programme. The average cost of books for students studying on a degree course is assumed as £100 per year.

Printing:
We recommend a minimum budget of £100 per year for printing costs including dissertation printing and binding. This relates to the printing of written documents through the photocopiers. Where relevant, the printing of artworks (draft and finished) will incur additional costs listed below.

In year or end of year exhibitions, projects and performances:
Where a course may contain exhibitions, activities, major projects or events additional costs will be incurred. These costs can be discussed in detail with your course teams and some will be linked to a professional skills element of the course where organised fundraising for such activities may be included. We would anticipate up to £100 per year maximum for these elements.

Graduation:
Graduation costs per student are estimated at £100 - £200 total. This is an optional cost for all students as attending graduation is not a requirement in order to have a degree conferred.

Hard Drive:
It is recommended that all students own a 1TB hard drive, or external storage drive.

Study Tours and Trips:
Optional trips and study tours of up to £100 per year. Students may wish to organise additional trips to support their own research of another £100.

Contact Hours

1 unit of credit is the equivalent of 10 notional learning hours. Full time undergraduate students study 120 credits (1200 hours) and full-time postgraduate students study 180 credits (1800 hours) per year or 'stage' of the course.

Course Stage	Scheduled Activities (Hours)	Guided Independent Study (Hours)	Placement / Study Abroad (Hours)
Year One	360	840	N/A
Year Two	360	840	N/A
Year Three	360	840	N/A
Year Four	360	840	N/A

Assessment Methods

The Assessment and Examination webpages provide further information on how assignments are marked and moderated, including a description of assessment activities. These also include further information about how feedback on assessed work is provided to students, including our commitment to ensure this is provided to students within 15 working days (the 'three-week turnaround').

The majority of the assessment within the MSci Cyber Security course comes from module coursework or team projects appropriate to the module itself. Module coursework will naturally vary across modules, but is likely to be representative of the following assessment types: essay writing; test, report writing; artefact construction (a technical design and development project using appropriate software and/or code); portfolio construction (task based, comprising report writing and the technical design/development of code or a software based artefact). Some modules will also make use of individual and group project presentations. So, a variety of assessment vehicles will be used as appropriate to the module, including assignments carried out in the student's own time, in-class assignment, workshops, presentations and formal examination. The form of assessment has been chosen so as to motivate students to achieve their best, and create learning activities for the students. The assessment vehicles for individual modules are detailed in the module descriptor.

Assessments will:

- Be appropriate to the task, achievable, motivating and vocationally focussed and will form a constructive part of the learning process.
- Develop general transferable skills as well as academic skills.
- Provide sufficient opportunity for the best students to exhibit a level of innovation and creativity associated with excellence.

Level 4 assessments will be primarily formative and will encourage the development of appropriate academic practice and concepts. The emphasis will be on frequent small-scale assessments wherever possible with a balance between formative and summative assessment.

Level 5 assessments will be more demanding, with the emphasis still on development of knowledge, skills, and concepts but now encouraging learning at greater depth, emphasising the fundamental principles. There will be a shift towards summative assessment.

Level 6 assessments are designed so as to allow students to demonstrate their knowledge and skills so that they have become effective, independent learners. The emphasis is on summative assessment.

Level 7 assessments are designed so as to allow students to critically further demonstrate their advanced knowledge and skills so that they have become leaders, effective, independent learners, and decision makers. The emphasis is on summative assessment.

Additional Assessment Regulations

- Students must achieve a minimum level average at Level 5 of 49.5% to progress into Level 6 of this Integrated Master's programme. Otherwise they will be transferred to the BSc (Hons) Cyber Security programme.
- Failure to achieve 120 credits at Level 6 of the Integrated Master's will also result in either transfer to the BSc (Hons) Cyber Security programme or consideration for an appropriate exit award.

Classification

Calculation of final award:	Level 6 - 33% / Level 7 – 67%

For full details of assessment regulations for all taught programmes please refer to our Results webpages. These include the criteria for degree classification.

Admissions Requirements

Please see the Application webpages for more information on how to apply, including a statement on how we support students from a variety of backgrounds. Please also see our general entry requirements for taught programmes. Applicants who do not meet our published entry requirements are encouraged to contact our admissions team for further advice and guidance.

Typical applicant profile and any programme-specific entry requirements

The aim of this honours programme is to ensure that graduates acquire knowledge and competence in cyber security and secure systems development, together with the underpinning theory of computer science. The course provides a balance of theory and practice in information technology, systems and software engineering, alongside providing a secure base for further development within the workplace. It is suitable for learners looking to develop themselves professionally, or who wish to return to or continue their education in a manner which will enhance their professional standing.

Opportunities for students on successful completion of the programme

Cyber Security graduates will have an in-deep understanding and knowledge of how to analyse and protect variant system applications against different threats and risks, and have the capability to consult on and develop security systems.

Graduates will be well placed to provide and manage solutions to security problems in systems and networks. There are multiple roles and careers available for those who have demonstrable capability in information and cyber security; and the award will allow graduates to enter the sector with confidence and evidence of subject specific knowledge and understanding. It follows that graduates will be more likely to be able to obtain employment in the component industries; and current employees will be better equipped to seek promotion and advancement. All graduates will have developed transferable skills that can be used in a wide range of employment roles.

The MSci in Cyber Security will enable graduates to take on a range of roles that include: System Security Specialists, Cyber Security Engineers, System Security Analyst/Architects, Information Analysts, or Architects.

The most common job titles, according to the SANS Institute Cybersecurity Professional Trends survey, are: Security Analyst, Security Engineer or Architect, Security/IT Director or Manager, CISO/CSO, Systems Administrator, Network Architect or Engineer, Forensics Investigator, Auditor, Systems Engineer or Integrator.

Recognition of Prior Learning

Previous study, professional and / or vocational experiences may be recognised as the equivalent learning experience and permit exemption from studying certain modules. Please refer to our Credit Accumulation webpages for further guidance.

Student Support

During the course of their studies, students will be supported in the following ways:

- At the start of their studies all students will receive a full **induction** to the programme which will include introduction to the staff responsible for delivering the course, and access to library and IT facilities
- The **Programme Handbook** will outline the exact nature of the course and how it is structured, including the availability of option modules
- Each student will be allocated a **Personal Tutor** who will support their academic development, be able to advise and guide them with their studies and, where necessary, give advice on study options
- Students will be able to access our full range of **support services**, including the Learning Development Unit for skills and study support, the Library, the Careers and Employability Team, Student Finance Team, Accommodation and Counselling Services

Appendices

Quality Assurance

Awarding Body:	**Buckinghamshire New University**
Language of Study:	**English**
QAA Subject Benchmark Statement(s):	**QAA Subject Benchmark Statement for: Computing (2019) Master's degrees in computing, 2019**
Assessment Regulations:	***Academic Assessment Regulations*, (https://bucks.ac.uk/students/academicadvice)**
Does the Fitness to Practise procedure apply to this programme?	**No**
Date Published / Updated:	**05 April 2020**

Other awards available on programme (Exit Qualifications)

Please refer to the *Academic Qualifications Framework* for Exit Qualifications recognised by the University and credit and module requirements.

Name of Exit Qualification:	**Certificate of Higher Education (CertHE)**
Full name of Qualification and Award Title:	**CHE Cyber Security**
Credits requirements:	**120 Credits**
Module requirements:	**120 Credits at Level 4**
Learning Outcome	
Identify global contemporary issues relating to Cyber Security techniques, and solutions	
Demonstrate critical consideration of key concepts, issues and theories related to the development, management and marketing of security businesses	
Critically evaluate arguments, assumptions, abstract concepts /data to make informed analysis	
Demonstrate a sound understanding of organisational information and system security requirements	
Describe the components of an effective operational security management plan	

Name of Exit Qualification:	**Diploma of Higher Education (DipHE)**
Full name of Qualification and Award Title:	**DHE Cyber Security**
Credits requirements:	**240 Credits**
Module requirements:	**ALL 120 Credits at Level 4 and 120 Credits at Level 5**
Learning Outcome	
Identify and discuss global contemporary issues relating to Cyber Security techniques, management, and solutions	
Demonstrate critical consideration of key concepts, management/marketing of security businesses	

Critically evaluate arguments, assumptions, abstract concepts /data to make informed judgments

Name of Exit Qualification:	**Ordinary Degree**
Full name of Qualification and Award Title:	**BSc Cyber Security**
Credits requirements:	**300 Credits**
Module requirements:	**ALL 120 Credits at L4 and 120 Credits at L5** • **60 credits from any two modules of CO654, CO652, CO669, CO666, CO651, CO655, CO670, CO653**
Learning Outcome	
Identify and discuss global contemporary issues relating to Cyber Security techniques, management, and solutions	
Demonstrate critical consideration of key concepts, issues and theories related to the implementation, management and marketing of security businesses	
Critically review and synthesise to execute a sustained piece of independent work using the media	
Critically describe the role and evaluate the significance of effective cyber security management in an organisational context	
Explain the contribution of cyber security management policy and practice in developing effective organisational and business strategies and how they provide the focus for a long-term approach to the effective development of the organisation	

Name of Exit Qualification:	**Honours Degree (bachelor's degrees)**
Full name of Qualification and Award Title:	**BSc (Hons) Cyber Security**
Credits requirements:	**360 Credits**
Module requirements:	**ALL 120 Credits at L4, 120 Credits at L5** • **90 credits from any 6 Level 6 modules CO654, CO652, CO669, CO666, CO651, CO655, CO670, CO653** • **CO701 (30 credits)***
Learning Outcome	
Identify and discuss global contemporary issues relating to Cyber Security techniques, management, and developed solutions	
Critically demonstrate the consideration of key concepts, issues and theories related to the development, management and marketing of security businesses	
Critically review, consolidate, and synthesise to execute a sustained piece of independent work using appropriate media	
Critically evaluate the consequences of organisational and personal behaviours, traits and motivation on effective threat risk and impact mitigation	
Design complex solutions for managing and configuring secure enterprise networks.	

* Students will only be required to undertake one dissertation, this will be located in L7.