University Centre Leeds

Programme Specification

1	**Awarding Institution/Body**	Luminate Education Group
2	**Delivery Location(s)**	University Centre
3	**Programme Externally Accredited by (e.g. PSRB)**	
4	**Award Title(s)**	Foundation Degree Cyber Security
5	**FHEQ Level** *[see guidance]*	5
6	**Bologna Cycle** *[see guidance]*	Short cycle
7	**HECoS Code and Description**	100366 Computer Science The study of the design and application of electronic computer systems, including computer architectures, software and systems design.
8	**Mode of Attendance** *[full-time or part-time]*	Full-Time or Part-Time
9	**Relevant QAA Subject Benchmarking Group(s)**	Computing 2019 Foundation Degree September 2015
10	**Relevant Additional External Reference Points** *(e.g. National Occupational Standards, PSRB Standards)*	National Occupational Standards: Technical Evaluation Level 5 Role -URN: ESKITP7125 Cyber Security Technical Professional Integrated Degree Apprenticeship (March 2020) QAA Characteristics Statement Higher Education in Apprenticeships (July 2019)
11	**Date of Approval/ Revision**	2020
12	**Criteria for Admission to the Programme (select the appropriate Entry Criteria for the award and remove the others)**	

<div align="center">

Foundation Degree Entry Criteria

</div>

	Typical offer	Minimum Offer

Level 3 qualifications such as: A Levels or BTEC L3 Diploma or Extended Diploma	48 UCAS tariff points from two A-levels (or equivalent qualifications)	16 UCAS tariff points from one A-level (or an equivalent qualification)
GCSE English: Desirable but not essential	English Language grade 4 or above. Key Skills Level 2, Functional Skills Level 2 and the Certificate in Adult Literacy are accepted in place of GCSEs.	
GCSE Maths:	Maths grade 4 or above. Key Skills Level 2, Functional Skills Level 2 and the Certificate in Adult Numeracy are accepted in place of GCSEs.	
IELTS:	IELTS 6.0 with no less than 5.5 in any component.	
International qualifications:	International qualifications will be assessed against these criteria	
Mature applicants:	University Centre Leeds welcomes applications from mature* applicants who may not have met the academic criteria, but who can demonstrate a wealth of experience in their chosen field. Candidates in this category and otherwise are likely to be interviewed to assess their suitability for the course and may be asked to provide a portfolio of evidence to support their application. *2*1 years and over at the start of the course*	
RPL claims:	The course structure actively supports claims for Recognition of Prior Certified Learning (RPCL) or Recognition of Prior Experiential Learning (RPEL)	

Additional entry criteria (to be added where applicable)	
	Criteria
Part Time:	Students applying for part time study are required to hold a full level 3 qualification or the equivalent experience in a relevant subject and will be working in the sector.
Apprentices:	In addition to the entry requirements of the academic programme, outlined above, apprentices must also meet the entry requirements laid out in the Cyber Security Technical Professional Integrated Degree Apprenticeship (March 2020). This states that individual employers will set the selection criteria, but this is likely to include three 'A' levels, including maths, or other relevant qualifications or experience.

13	**Educational Aims of the Programme**

The overall aims of the programme are to:
- Provide a comprehensive and challenging vocational programme in cyber security, including core and specialist modules, which facilitate access and progression for a wide range of students from diverse backgrounds into various computer/digital industry contexts.
- Offer a robust Foundation Degree programme that is relevant to current practice in the cyber security industry that will allow students to be autonomous and progress onto their chosen trajectory.
- Produce graduates who have the ability to critically reflect and learn from their practical and academic experience in a computing context and relate this experience to relevant theory.
- Produce graduates who have both subject specific skills (expressive, creative, technical) and professional, interpersonal, business and transferable skills (communication, teamwork,

	project management) which are key to being employable within the computing/digital industry.
	● Produce graduates with entrepreneurial ability relevant to the cyber security industry
	● Produce graduates who have an analytical and reflective understanding of cyber security, its significance, concepts, threats, vulnerabilities and assurance, as well as wider digital subjects in the context of the workplace today and in relation to the wider social and cultural environment.

14	**Learning Outcomes**
	The programme will enable students to develop the knowledge and skills listed below. On successful completion of the programme, the student will be able to:
	Knowledge and Understanding *(insert additional rows as necessary)*
	K1 — Evaluate the relevant theories, concepts and principles applicable to cyber security
	K2 — Identify and use appropriate research methods in the context of cyber security
	K3 — Evaluate the legal and ethical issues and the expectations of users in relation to computing practice
	Cognitive/Intellectual Skills *(insert additional rows as necessary)*
	C1 — Apply problem solving and solution-based methodologies to the development of cyber security systems
	C2 — Analyse, interpret and use data from a variety of sources
	C3 — Use balanced and logical arguments to resolve given questions, scenarios and case studies
	C4 — Select appropriate tools and techniques for the development and implementation of cyber security solutions
	Practical/Professional Skills *(insert additional rows as necessary)*
	P1 — Apply a range of practical skills in the context of cyber security systems and applications
	P2 — Develop usable solutions using appropriate software, programming languages and/or design concepts
	P3 — Effectively integrate a range of practical computing techniques
	P4 — Integrate the expectation of users and appreciation of legal and ethical issues when developing a computing solution
	Key Transferable Skills *(insert additional rows as necessary)*
	T1 — Reflect systematically on your approach and performance to further develop learning.
	T2 — Act with increasing autonomy with reduced need for supervision and direction, within defined guidelines
	T3 — Communicate accurately using a range of communication methods appropriate to the context
	T4 — Demonstrate creativity, innovation and independent thinking
15	**Key Learning & Teaching Strategy and Methods**
	The learning and teaching strategy and methods employed throughout the course are designed to support students in meeting the learning outcomes by offering a range of opportunities, including individual and group practical and research projects, written and oral forms of presentation and the creation of cyber security development work.
	Cyber Security engages with a wide range of teaching methods: practical workshops, lectures, seminars, large and small group discussion and presentations, it is, therefore, inclusive for a variety of learning styles.
	Each module states a range of learning and teaching methods used for its delivery.
	Teaching and Learning strategies will include lectures, one to one and group discussions. Individual consultations will underpin each module where such things as guidance on writing and presenting an effective brief and project proposals will be covered, as well as practical support.

The programme will provide support to allow students to work autonomously, with structured guidance from lecturers, project or task milestones will be agreed to track progress to support the transition to working more autonomously, especially at Level 4.

Guidance on working towards recognised industry practice will be provided through real world case studies. The simulation of industry practice will be embedded in the programme to develop independent working processes and approaches through the development of viable Cyber Security projects and theoretical analysis and application.

Lectures, practical demonstrations and discussion will be delivered that are pertinent to the particular module. Guidance on research procedures and methodologies will be embedded alongside academic skills development to ensure students written work is up to the acceptable academic standards expected at this level of study.

One to one tutorials will be used to provide guidance and practical support to produce working Cyber Security projects and prototypes to professional standards and encourages the realisation of a range of practical skills in Cyber Security. Individual and small group consultations will be utilised to develop wider contextual understanding of how small teams of developers produce computing solutions in a range of contexts, through devising and developing practical projects.

A range of formative and summative assessment strategies that will include, questioning, open ended questions, brainstorming, presentations, production diaries, work logs, observations, self-assessment, group discussion, peer assessment, questionnaires, reflective practice.

e-learning strategy
The programme will incorporate the use of Google Classroom where module resources will be uploaded. Students will be able to access all materials on or off-site, this will enable students to better fit their learning around their lifestyles and manage other commitments.

Using google classroom will allow staff to employ a range of tools to enhance the learning experience and will include online discussions, tutorial videos, links to module specific online video and podcasts

All assignments will be set in google classroom and students will upload their final submissions to google classroom or via turnitin for written submissions. The methods and platform of submission will be clearly stated and reinforced in each module handbook and during delivery of that module.

Staff can engage with students outside of class using google classroom to provide a broader range of support for students. This will also include a learning community via a Facebook group where students can engage with one another to help, support and share resources.

Work Related Learning and Personal Development
There are no requirements for a formalised work placement but the programme has a focus on preparing students for work in the Cyber Security industry. This is done mainly through the simulation of industry working practices. Students are encouraged to work collaboratively in specified modules at L4 and L5, forming small development teams that are reflective of the makeup of real-world development teams.

Hackathons, Code Clubs and Game Jams are also a focus on the course and students will take part in a number of these events at L4 and L5 of the programme. These will provide Cyber Security students with the opportunity to broaden their skills base and potential employment routes. There are a number of external Game Jams that students will take part in, the global Game Jam for example, a weekend

long global competition where students will work towards developing a rapidly developed prototype based on a given theme.

The programme endeavours to develop students with an enthusiasm for enquiry into their discipline and the motivation to sustain it. Currently this happens in many guises, the practical focus of the course is key to student buy in, as is the development of a collaborative atmosphere. Students are encouraged to use out of class time to socially interact through playing games, code clubs and hackathons within the University Centre to maintain enthusiasm for the subject.

Employability is embedded in to the programme and this will be underpinned with the development of an online portfolio and also through a scheme of visiting lecturers and industry practitioners who will provide insight and also portfolio advice, guidance and critique where appropriate.

The employability module will provide the opportunity to develop a broad range of employability skills, often pitched as "soft Skills". These will include the ability to think creatively, work individually or as part of a team, strategic thinking, plan and prepare budgets, chair and contribute to meeting, positive work ethic with good punctuality, excellent written and verbal communication skills.

Wider technical employability skills are embedded in practical modules that will reflect industry practice as closely as possible. There are also group/small team projects that are designed to simulate industry practice in the development of team-based business solutions that will focus on solving identified problems with a technical solution relevant to the discipline.

There is also opportunity for interdisciplinary work to take place with collaboration between Computer Games students a possibility. The L5 project module is also part of the Computer Games courses and is planned to at the same time as the project module on the Computing courses.

The strategies outlined here are also applicable to the Cyber Security Technical Professional Integrated Degree Apprenticeship route being offered. The practical nature of the learning and teaching strategy and methods lends itself well to developing the technical competencies and set out in the apprenticeship standard.

Technical knowledge and understanding, as well as professional, interpersonal and business skills, are further developed through individual and group practical and research projects, written and oral forms of presentation and the creation of cyber security development work. In particular, the strategy adopted allows for the development of skills related to written communications, well-structured verbal presentations and arguments, effective working with others, effective research, and creative approaches to problem solving.

An underpinning focus on critical reflection, reflective practice, and personal and professional development will provide apprentices an opportunity to identify their own, and others, preferences, motivations, strengths and limitations, with application of insight to more effective individual and team working. Within this is the development of being able to provide constructive feedback to peers as well as working closely with module tutors, pastoral tutors and peers to welcome feedback to be incorporated into his/her own professional development and life-long learning.

Further, throughout the whole programme, the behaviours outlined in the standard are developed on programme as well as in the workplace, and reflect the educational aim of producing graduates with entrepreneurial ability relevant to the cyber security industry.

16	**Key Assessment Strategy and Methods**

Employability is built into the programme in core modules. Future employment is entrenched within the programme and practical modules are very much focused on the development of professional portfolio pieces that can support progression in to employment.

Wider technical employability skills are embedded in practical modules, the assessments have been selected to reflect industry practice. These projects will focus on solving identified business problems with a technical solution that is relevant to the specific programme discipline.

Small team projects have been designed to simulate industry practice in the development of team-based business solutions. Identifying roles and undertaking these roles in a team setting are essential skills and key to the overall teaching strategy, in respect of preparing students for employment.

There is also opportunity for interdisciplinary work to take place with collaboration between Computer Games students a possibility. The L5 project module is also part of the Computer Games courses and is planned to at the same time as the project module on the Computing courses.

A broad range of skills and knowledge are needed in the Cyber Security and digital sectors and assessments are tailored to the particular task being undertaken. Assessed tasks include the development of computing solutions for real-world problems, the application of theory to problem solving and practical problems, team work, project work and the communication of ideas and concepts through reports and presentations. The assessment of these tasks are guided by programme and module learning outcomes.

Each module will have two assessment components. Programme learning outcomes will be assessed twice giving ample opportunity for students to meet the specified learning outcomes of each task and will also ensure that module learning are only assessed once.

Assignments tasks will be managed across the academic year ensuring there is sufficient time between assessments to support the completion of the programme.

The course promotes independent learning through the promotion of CPD when learning new software and when researching and applying new theories and concepts. Students are encouraged to adopt an analytical approach to their engagement with Cyber Security, transitioning from user to developer and analyst by applying a critical eye to key computing skills development and independently applying new found approaches to their own computing solutions and concepts. Greater autonomy is expected as students move from L4 to L5 of the programme and this is supported through the exploration, experimentation, development and application of key theories and practice in their coursework.

Formative assessments usually carry no weighting but are critical for the student's development and can be useful preparation for the related summative assessment. Formative assessment can take the form of a group or individual critique, and informal peer assessment through peer group discussions.

Formative assessment is a part of the individual tutorial system, featured in every module, and feedback is given verbally or in written format depending on the module. Each assessment is aligned with its intended learning outcomes and learning activities, so it is clear what is being assessed.

Formative assessment is a key feature of the first year and will be the focus of group tutorials during the induction period to familiarise students with the formative feedback strategy.

Summative feedback will be given in written format using standard programme feedback forms. The feedback will discuss the final grade decision and how it was reached and also offer feedforward style

feedback that will identify areas for improvement and suggest approaches that can be adopted in future assessments. This will help students to identify areas for improvement, and of current strengths which are to be developed.

All feedback will be presented in line with the institution's policy ensuring timely feedback is given to students for each assessment.

More specifically related to apprentices, the key assessment strategy and methods outlined above closely reflect the skills and behaviours required in the workplace and by a cyber security technical professional. A number of competencies, knowledge and underpinning skills attitudes and behaviours have been identified within the apprenticeship standard. These consider; technical competencies; written communications; well-structured verbal presentations and arguments; effective working with others; effective research; creative approaches to problem solving; a demonstration of business disciplines, ethics and courtesies; an ability to perform under pressure; and a thorough approach to work in the cyber security role. An appreciation of these has been considered in the assessment strategy and methods and the examples above illustrate how the approach fully supports the apprentice in both succeeding in the academic programme but also in the completion of their apprenticeship.

There will be continuous assessment of competencies from the outset of the programme and beyond completion of the degree to end point assessment (EPA). This is to be completed within three months of completing the BSc (Hons) programme of which this Foundation degree is Level 4 and 5 or Year 1 and 2. The apprentice will be considered for the EPA on meeting the requirements of the EPA gateway, these being:
- employer confirmation that the apprentice is ready for the EPA and has met the knowledge, skills and behaviour requirements set out in the occupational standard (based on work-based performance);
- completion and passing of all modules;
- passing of Level 2 English and maths (if not already achieved);
- production of a portfolio in relation to the knowledge, skills and behaviours for the technical discussion of the EPA.

The curriculum team, and the employer will support the apprentice in building their portfolio, with the opportunities to develop the skills for and to work on real work projects completed in the workplace and as part of the key learning, teaching and assessment strategies and methods providing evidence to be presented within the portfolio. It will also include peer feedback and of evidence of team working. This may take the form of text, graphics, presentations, spreadsheets, project plans, the product itself (such as a piece of code), job sheets, case studies, screen dumps, links, photographs, audio, video, written feedback. All these forms of evidence are included in the key learning, teaching and assessment strategy and methods, whether that be formative or summative and so demonstrates how the programme supports the apprentice fully in their portfolio development.

The EPA itself consists of a practical test and a technical discussion (informed by the portfolio). The practical nature of the course, as well as the assessment methods of the programme, compliments the skills and knowledge developed in the workplace to further advance competencies required for the practical tests. In addition to this, the development of communication skills throughout the programme, with a demonstration of these in written and verbal form throughout the modules, further supports the apprentice for the technical discussion. There will be additional tutorial time with an assessor at the end of each academic year to support preparation for the EPA.

See mapping document (pg18) for see examples of where evidence/content for the EPA is being developed throughout the programme.

17	**Programme Modules**						

Level

Code	Title	Credits	Core/ Option	Non-Compensatable	Compensatable	Variance
	Networks	20	Core		Yes	
	Principles of Cyber Security	20	Core		Yes	
	Principles of Databases	20	Core		Yes	
	Principles of Programming	20	Core		Yes	
	Professional Development	20	Core		Yes	
	Web and Apps	20	Core		Yes	

Level 5

Code	Title	Credits	Core/ Option	Non-Compensatable	Compensatable	Variance
	Linux and Scripting	20	Core		Yes	
	Computer Forensics	20	Core		Yes	
	Employability Skills	20	Core		Yes	
	Ethics and Ethical Hacking	20	Core		Yes	
	Securing Networks	20	Core		Yes	
	Project	20	Core		Yes	

18	Programme Structure

Cyber Security Full-Time

Level 4				
Semester One	**Principles of Programming** (20 Credits)	**Web and Apps** (20 Credits)	**Networks** (20 Credits)	**Professional Development** (20 Credits)
Semester Two		**Principles of Databases** (20 Credits)	**Principles of Cyber Security** (20 Credits)	

Level 5			
Semester One	**Linux and Scripting** (20 Credits)	**Computer Forensics** (20 Credits)	**Employability Skills** (20 Credits)
Semester Two	**Ethics and Ethical Hacking** (20 Credits)	**Securing Networks** (20 Credits)	**Project** (20 Credits)

Cyber Security Part-Time

Level 4				
Year One	**Principles of Programming** (20 Credits)	**Web and Apps** (20 Credits)	**Networks** (20 Credits)	**Professional Development** (20 Credits)
Year Two		**Principles of Databases** (20 Credits)	**Principles of Cyber Security** (20 Credits)	

Level 5			
Year Three	**Linux and Scripting** (20 Credits)	**Computer Forensics** (20 Credits)	**Employability Skills** (20 Credits)
Year Four	**Ethics and Ethical Hacking** (20 Credits)	**Securing Networks** (20 Credits)	**Project** (20 Credits)

The Foundation Degree is awarded on successful completion of both level 4 and level 5 of the award.

The course is full-time, students studying on the foundation degree full time will attend college for 2 days per week. Students, alongside core modules will have a tutorial which will have a study support theme.

The Part-time option will see students attend college for 1 day per week over 4 years.

At Level 4 all modules are delivered in either semester 1 or semester 2 with the exception of Principles of Programming which is delivered across both semesters. This will ensure that skills are developed sequentially and will be enhanced over the academic year. For example, in semester 1, the mark-up programming language used in the Web and Apps module will introduce students to writing code that will inform and underpin skills they will be developing in the Principles of Programming module. This will also ensure that skills in semester one will feed in to modules in semester two. In addition, having the Networks module in the first semester will provide the network infrastructure knowledge to better understand the principles of Cyber Security in respect of ensuring networks are not vulnerable to attack.

At Level 5 all modules are delivered in either semester 1 or semester 2. The sequence of modules is designed to provide the practical tools in one module that will be used in the proceeding module. For example, the skills learnt in computer forensics will be further developed and applied in the ethics and ethical hacking module. Thus, providing further opportunity to implement computer forensics skills developed in ethics and ethical hacking in a different context.

Cyber Security Technical Professional Apprentices
The Cyber Security Technical Professional Integrated Degree Apprenticeship has a typical duration of 48 months (not including the EPA period) with 20% off-the-job training. In line with this, the programme structure for apprentices is one day per week over 45 weeks. Apprentices will infill with full time students one day per week in Semester 1 (weeks 1-15) and Semester 2 (weeks 16-30) and then one day per week as an apprenticeship only cohort for a Semester 3 (weeks 31-45). Level 4 will take one year (45 weeks) to complete. Level 5 will also take one year, essentially year 2 of programme.

Level 4			
Semester One	**Principles of Programming** (20 Credits)	**Web and Apps** (20 Credits)	**Networks** (20 Credits)
Semester Two		**Principles of Cyber Security** (20 Credits)	**Portfolio Development and one-to-one support**
Semester Three	**Professional Development** (20 Credits)	**Principles of Databases** (20 Credits)	

Level 5			
Semester One	**Linux and Scripting** (20 Credits)	**Computer Forensics** (20 Credits)	**Portfolio Development and one-to-one support**
Semester Two	**Ethics and Ethical Hacking** (20 Credits)	**Securing Networks** (20 Credits)	

Semester Three	Employability Skills (20 Credits)	Project (20 Credits)		

In order to achieve the apprenticeship, apprentices must then progress onto level 6 and successfully complete the BSc (Hons) Cyber Security Technical Professional (top-up). This will take one year (45 weeks) and so year 3 of programme.

All modules will help support the development of technical knowledge and/or practical skills relevant to the practical test of the EPA. The Project completed in Semester 3 (weeks 31-45) will be focussed on a real work project relevant to the apprentices and will providing robust evidence to be presented within the portfolio. It will help form the basis of the technical discussion of the EPA as well as further supporting the development of technical competencies, technical knowledge, and underpinning professional, interpersonal, business skills, and behaviours set out in the apprenticeship standard. The level 5 Project also acts as a preparatory and developmental module leading to the Dissertation at level 6. Both the Project and the Dissertation are devised to meet the requirements of the academic programme as well as the requirements of the EPA gateway and the EPA itself. They, and the other modules included in the programme, will draw on the apprentice's current work practices and real work projects. Here, the apprenticeship requirements below will clearly be developed and evidenced:
- analytical and critical thinking,
- systematic analysis and application of structured problem-solving techniques to complex systems and situations,
- conducting effective research using literature, fluent written communications articulating complex issues, and
- making concise, engaging and well-structured verbal presentations, arguments and explanations.

| 19 | **Apprenticeships**
The foundation degree programme, with the BSc (Hons) Cyber Security Technical Professional (top-up), can be completed to support the achievement of the Cyber Security Technical Professional Integrated Degree Apprenticeship (March 2020). Aligning with the QAA Characteristics Statement Higher Education in Apprenticeships (July 2019), this relates to 2.4 Progression by providing transparent ongoing career progression from level 3 and 4 apprenticeships being offered within the locality, and facilitating opportunities for progression into an apprenticeship at a higher level and into studies at a higher level. It also supports section 2.3 Accessibility in terms of acting as a means to increasing social mobility and access into further and higher education.

During the recruitment process, the curriculum team/assessor and employer will work together to agree the delivery model for the apprentice. There will be discussion of any prior learning, the apprentice's role and work practices in the workplace, and an identification of where the knowledge, skills and behaviours of the apprenticeship will be developed and evidenced both on programme and in the workplace.

The intention is that the apprenticeship will be delivered in a day release model over a period of 3 years where students will complete 120 credits per year of study. This will comprise two years of foundation degree and one year of BSc (Hons), each year including 45 weeks of delivery. Additional tutorial time with an assessor at the end of each academic year will be provided to ensure apprentices are fully supported in the development of the |
|---|---|

		portfolio and in preparing for the practical test and technical discussion of the EPA. Following these 3 years there will be additional support preparation on the completion of the EPA within 3 months of completing the degree. Throughout the programme there will be an inclusion of one-to-one support for apprentices in preparation of the portfolio and for the practical test and technical discussion of the EPA. There will also be close working and reviews with the employer to ensure the knowledge, skills and behaviours being developed on the academic programme are well timed and complimentary to the knowledge, skills and behaviours being developed in the workplace. The platform OneFile will be used to collate evidence for the portfolio as well as records of reviews and assessor tutorials. Support for apprentices begins at recruitment where they complete initial tests. Induction contains an introduction to the structure and regulations of the course in addition to a skills scan and advice on academic skills and library support (with research and referencing). It also covers workplace aspects such as code of conduct, one-file, health and safety, British Values/Prevent, and Safeguarding. Apprentices receive individual support through tutorial and are assigned a pastoral tutor. All students have access to welfare and may access academic and specialist support through a Coaching Tutor. The VLE supports students with further resources and extension and is available 24/7 anywhere with internet access. Employers, apprentices and workplace mentors will also receive a supporting handbook and the curriculum/assessor, apprentice and employer will have regular tracking meetings and progress reviews to ensure progress and support needs are well monitored. Students are taught in specialist suites using a mixture of lecture, practical and workshop activities with access to specialist tutorial and additional resources including the course textbook and VLE sites. Tutors on the programme are highly qualified and experienced subject specialists with industry experience. The key learning, teaching and assessment strategies have been articulated in the previous sections, all supported by ongoing support for the development of the portfolio for the EPA gateway. The development of the knowledge, skills and behaviours of the apprenticeship will be developed and evidenced throughout the programme and to support successful completion of the practical test and technical discussion (informed by the portfolio) of the EPA following completion of the degree programme.
20		**Support for Students and Their Learning** The award adopts the following approach to student learning support. ● Tailored induction to support the transition in to Higher Education ● A robust communications system functions to give students access to lecturers and management; this includes e-mail, the VLE and notice boards and open office policy. ● All necessary information about the programme is provided by means of the student handbook, module handbooks and the VLE. ● Each student is allocated a personal tutor for regular tutorials and personal development planning. This is implemented in the first term and continued throughout the year of study.

- Formative submissions outlined in course scheme of work and formative feedback given for each module component.
- Practical work supported by regular peer feedback through workshop critiques.
- Shared documents and folders between staff and students to support live editing and feedback on work.
- There is an extensive range of learning resources in the Library, supported by specialist staff that provide bespoke study skills sessions for students.
- The University Centre provides an extensive range of services for students, including support for those with special needs, welfare, counselling, financial and careers advice
- There are a range of student services such as welfare, counselling, financial and careers advice.
- Employability embedded throughout the programme

Students will be given a Chromebook or an equivalently priced laptop if they prefer when they start the course. There will be an option for students to upgrade this to a more powerful laptop if they agree to pay a supplement that will make up the difference in the cost of a Chromebook and the more powerful laptop. This cost will be reviewed yearly to reflect the changes in cost of devices year on year. The Chromebook or laptop will be required to last students the full duration of the course.

The department has a coaching tutor employed to support students and their learning. The coaching tutor will provide support in academic, technical and personal settings. The coaching tutor will also support students with deadlines, applying for short extension and mitigation and will also track and chase low attendance and engagement.

Personal tutorials will be carried out by the coaching tutor, these meetings will provide regular one to one support. Discussions will be logged and shared with module tutors to identify potential problems but to also highlight and share praise for excellent performance on module tasks.

The coaching tutor will act as the go to person for support. This will provide consistency for students with a clearly support staff who will get to know the students and their individual support needs.

Support for apprentices begins at recruitment where students are invited to an information session followed by an interview where they also complete initial tests. Induction contains an introduction to the structure and regulations of the course in addition to a skills scan and advice on academic skills and library support (with research and referencing). For apprentices the Apprenticeship Team also cover workplace aspects such as code of conduct, one-file, health and safety, British Values/Prevent, and Safeguarding.

Apprentices will receive individual support through tutorial and are assigned a pastoral tutor. By offering a day release model, apprentices will have a comparative experience to full time and non-apprentice students, being able access to additional learning support, welfare, counselling and academic and specialist support through a Coaching Tutor. This will also be accessible throughout weeks 30-45 where non-apprentice students are typically finished for the summer period. The VLE supports apprentices with further resources and extension and is available 24/7 anywhere with internet access.

	Apprentices will receive additional support in the workplace through mentors and assessors. Apprentices and workplace mentors will also receive a supporting handbook and the curriculum/assessor, apprentice and employer will have regular tracking meetings and progress reviews to ensure progress and support needs are well monitored. Structures support for preparation for the EPA is built into the apprenticeship timetable.	
21	**Distinctive Features** The newly formed Digital and Engineering department is uniquely positioned to offer excellent opportunities to students on our programmes. The provision in the department includes, Computing, Computer Games and Engineering programmes. This pack of courses offers exciting opportunities for collaborative work between students and staff. The cross over between the different disciplines outlined are numerous. The aim of the programmes is to have cross collaboration across all levels. Examples of the opportunities are to have Computing students who will have computer programming skills to work with Game Development students who will have 3D modelling and game level design skills, the potential outcomes are fully working prototype games. The Engineering industry are requiring more digital skills in manufacturing, automation and 3D product visualisations. Computing tutors are fully skilled in the topics of 3D modelling and could port these skills in to Computer Aided Design. Engineering staff could deliver Maths and Science based topics to Cyber Security students. These staff skills and knowledge place the department in a unique position to deliver modern programmes that are reflective of industry needs and practices. All courses are delivered on the same floor with teaching spaces that will easily facilitate collaborative opportunities. There are shared modules at both L4 and L5 on the Computing and Computer Games programmes to further facilitate collaborative opportunities. Timetables will be synchronised to support these opportunities. The focus of the programme is preparing students for a career in the computing and digital sector, either as a self-employed practitioner or as an employee of an SME or large-scale company. There is an overall emphasis on work related learning that reflects industry practice. Work related progression is the focus of two modules (Professional Development and Employability) with the aim of developing professionalism and preparing graduates for the world of employment in the sector. The first year of the course is designed to provide a range of principle skills that are broadly required across the computing and digital sectors. The institution currently offers computing and digital related studies from Level 1 to level 6, this supports students who develop better in a familiar environment with staff they know to achieve their full potential in a supportive environment. A focus of the programme is the development of practical skills that will form the foundation of a varied portfolio and are a valuable resource to demonstrate practical experience to employers.	

There is also a focus on developing personal and employability skills that are fast becoming required by employers in addition to practical skills. These skills often termed as "soft Skills" are embedded in the programme and as also in modules at level 4 and level 5.

There is a strong teaching team with links to industry that brings opportunity to students and the provision of real experience of working within the industry is embedded throughout the programme through simulation of practice and a series of guest lectures.

The department has a good working relationship with the institution's ITSS department, who have provided advice and guidance on module content. The ITSS department are also open to providing 2nd year students with the opportunity of short-term voluntary work experience. This is not a requirement of the course in terms of assessment and achievement but is encouraged if students have the time to fit work experience around course, home and personal commitments.

Stage Outcomes (Undergraduate Awards only)

No.	Programme Outcome	Stage/Level 4(1)
K1	Evaluate the relevant theories, concepts and principles applicable to cyber security	Describe and discuss concepts and principles applicable to cyber security
K2	Identify and use appropriate research methods in the context of Cyber Security	Use appropriate research methods in the context of Cyber Security
K3	Evaluate the legal and ethical issues and the expectations of users in relation to computing practice	Describe key legal and ethical issues and the expectation of users in relation to computing practice.
No.	**Programme Outcome**	**Stage/Level 4(1)**
C1	Apply problem solving and solution-based methodologies to the development of cyber security systems	Use problem solving methodologies to the development of cyber security systems
C2	Analyse, interpret and use data from a variety of sources	Use data from a variety of appropriate sources in defined contexts
C3	Use balanced and logical arguments to resolve given questions, scenarios and case studies	Resolve given questions, scenarios and case studies
C4	Select appropriate tools and techniques for the development and implementation of cyber security solutions	Use tools and techniques for the development and implementation of cyber security solutions
No.	**Programme Outcome**	**Stage/Level 4(1)**
P1	Apply a range of practical skills in the context of cyber security systems and applications	Demonstrate practical skills in the context of cyber security systems and applications
P2	Develop usable solutions using appropriate software, programming languages and/or design concepts	Apply solutions using appropriate software, programming languages and/or design concepts in defined contexts
P3	Effectively integrate a range of practical computing techniques	Integrate a range of practical computing techniques
P4	Integrate the expectation of users and appreciation of legal and ethical issues when developing a computing solution	Appreciate the expectations of users and legal and ethical issues when developing a computing solution
No.	**Programme Outcome**	**Stage/Level 4(1)**

T1	Reflect systematically on your approach and performance to further develop learning.	identify your own strengths and weaknesses to develop learning
T2	Act with increasing autonomy with reduced need for supervision and direction, within defined guidelines	Act with limited autonomy with reduced need for supervision and direction, within clearly defined contexts
T3	Communicate accurately using a range of communication methods appropriate to the context	Use a range of communication methods appropriate to the context
T4	Demonstrate creativity, innovation and independent thinking	Demonstrate creativity within clearly defined contexts

Key: **K** = Knowledge and Understanding **C** = Cognitive and Intellectual **P** = Practical Professional **T** = Key Transferable [*see Section 16 programme specification*]

Map of Outcomes to Modules

Level 4														
Outcome Key														
Module Titles	K1	K2	K3	C1	C2	C3	C4	P1	P2	P3	P4	T1	T2	T3	T4
Principles of Programming		✓			✓	✓			✓						✓
Web and Apps				✓				✓	✓			✓	✓		
Principles of Databases		✓			✓	✓				✓	✓				
Networks	✓						✓	✓					✓		
Principles of Cyber Security	✓		✓	✓						✓	✓			✓	
Professional Development			✓				✓					✓		✓	✓

Level 5														
Outcome Key														
Module Titles	K1	K2	K3	C1	C2	C3	C4	P1	P2	P3	P4	T1	T2	T3	T4
Linux and Scripting			✓				✓		✓	✓		✓			
Ethics and Ethical Hacking	✓			✓	✓				✓						✓
Computer Forensics	✓				✓	✓				✓					✓
Securing Networks				✓		✓		✓			✓		✓		
Employability Skills		✓					✓						✓	✓	
Project		✓	✓					✓			✓		✓	✓	

	Map of Teaching and Learning Methods

Level 4

Module Titles	Lectures	Student led/ interactive/ shared learning seminars	Case Studies	Skills workshops	Practical's (design and production sessions)	Group activities	Guest speakers	Independent / E Learning/ On-line forums
Principles of Programming	✔	✔	✔	✔	✔			✔
Web and Apps	✔	✔		✔	✔			✔
Principles of Databases	✔	✔			✔			✔
Networks	✔	✔	✔		✔	✔	✔	✔
Principles of Cyber Security	✔	✔			✔		✔	✔
Professional Development	✔	✔	✔		✔			✔

Level 5

Module Titles	Cyber Security L5							
	Methods							
Module Titles	Lectures	Student led/ interactive/ shared learning seminars	Case Studies	Skills workshops	Practical's (design and production sessions)	Group activities	Guest speakers	Independent / E Learning/ On-line forums
Linux and Scripting	✔	✔	✔	✔	✔			✔
Ethics and Ethical Hacking	✔	✔		✔	✔			✔
Computer Forensics	✔	✔			✔			✔
Securing Networks	✔	✔			✔	✔	✔	✔
Employability Skills	✔	✔	✔	✔			✔	✔
Project	✔	✔	✔		✔	✔		✔

Map of Assessment Methods

Level 4

		Methods

Module Titles	Report	Programming Portfolio	Practical	Evaluation	Presentation	Evaluative Response
Principles of Programming	40% (1200 Words) Wk 29	60% (1800 Words) Wk 27				
Web and Apps			70% (2100 Words) WK 13	30% (900 Words) WK 14		
Principles of Databases			70% (2100 Words) WK 28 WK 43 for apprentices	30% (900 Words) WK 29 WK 44 for apprentices		
Networks	30% (900 Words) Wk 9		70% (2100 Words) Wk 15			
Principles of Cyber Security	60% (1800 Words) Wk 24		40% (1200 Words) Wk 30			
Professional Development					40% (1200 Words) Wk 26	60% (1800 Words) Wk 17

Level 5

Module Titles	Methods							
	Report	Practical	Blog/Vlog	Practical Logbook	Case Study	Interview and Pitch	Practical Project	Reflection
Linux and Scripting	30%(1200 Words) Wk 14	70% (2800 Words) Wk 15						
Ethics and Ethical Hacking	40% (1600 Words) Wk 20	60% (2400 Words) Wk 27						
Computer Forensics	30% (1200 Words) Wk 22			70% (2800 Words) Wk 29				

Module									
Securing Networks		70% (2800 Words) Wk 26	30% (1200 Words) Wk 24						
Employability Skills					40% (1600 Words) Wk 10 WK 40 for apprentices	60% (2400 Words) Wk 13 WK 43 for apprentices			
Project								70% (2800 Words) Wk 28 WK 43 for apprentices	30% (1200 Words) Wk 30 WK 45 for apprentices

Cyber Security Technical Professional Integrated Degree Apprenticeship (March 2020) Mapping

Modules/ Technical Knowledge and Understanding	Networks	Principles of Cyber Security	Principles of Databases	Principles of Programming	Professional Development	Web and Apps	Linux and Scripting	Computer Forensics	Employability Skills	Ethics and Ethical Hacking	Securing Networks	Project
Foundations of cyber security, its significance, concepts, threats, vulnerabilities and assurance.		?					?				?	
Network foundations, connections, internetworking, protocols, standards, performance, security and server virtualisation.	?										?	
Information management, big data concepts, statistical techniques, database concepts and data quality.	?		?									

Computer architecture, digital logic, machine level representation of data.	☐										
Operating System principles, architectures, features, mechanisms, security features and exploits.	☐						☐				
Algorithm and program design, concepts, compilers and logic. Programming languages.				☐			☐				
Algorithms, complexity and discrete maths.	☐			☐							
How software interacts with the hardware and real world environment and security issues.	☐							☐		☐	
Malware, reverse engineering, obfuscation.								☐		☐	☐
Defensive programming, malware resistance, code analysis, formal methods, good practice.				☐						☐	☐
System development principles, tools, approaches, complexity, software engineering.				☐			☐				
Threats, vulnerabilities, impacts and mitigations in ICT systems and the enterprise environment.		☐					☐	☐			☐
Human dimensions of cyber security.									☐		
Structured and ethical intelligence analysis, methods, techniques.		☐			☐			☐			
Management of cyber security risk, tools and techniques.		☐			☐						☐

Learning Outcome	1	2	3	4	5	6	7	8	9	10	11	12	13
Quantitative & qualitative risk management theory & practice, role of risk stakeholders.	✓											✓	
Concepts & benefits of security management systems, governance & international standards.	✓							✓				✓	
Security components: how they are used for security / business benefit. Crypto & key management.	✓	✓									✓	✓	
How to compose a justified security case.	✓						✓				✓	✓	✓
Understand security assurance, how to achieve it and how to apply security principles	✓	✓									✓	✓	
Assurance concepts & approaches.		✓						✓				✓	✓
How to diagnose cause from observables. Application of SIEM (Security Information and Event Management) tools & techniques.	✓							✓				✓	
Cyber incident response, management, escalation, investigation & 3rd party involvement.	✓							✓				✓	
Legal, regulatory, compliance & standards environment.		✓			✓					✓			
Applicability of laws regulations & ethical standards.		✓						✓		✓			
Legal responsibilities of system owners, users, employers, employees.					✓				✓	✓			✓

Modules/ Technical Competencies	Networks	Principles of Cyber Security	Principles of Databases	Principles of Programming	Professional Development	Web and Apps	Linux and Scripting	Computer Forensics	Employability Skills	Ethics and Ethical Hacking	Securing Networks	Project
Design, build, configure, optimise, test and troubleshoot simple and complex networks.	?										?	
Apply statistical techniques to large data sets. Identify vulnerabilities in big data architectures and deployment.	?		?									
Build test and debug a digital system to a specification.	?											
Configure an Operating System in accordance with security policy. Identify threats and features.	?						?					
Write, test, debug programs in high and low level languages and scripts.				?			?					
Design, implement and analyse algorithms.	?			?								
Construct software to interact with the real world and analyse for security exploits.	?							?			?	
Analyse malware & identify its mechanisms.								?		?	?	
Apply secure programming principles and design patterns to address security issues.				?						?	?	
Apply system engineering and software development methodologies and models.				?			?					

Programme Spec – FD Cyber Security
Version 3 – August 2023

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14
Discover, identify and analyse threats, attack techniques, vulnerabilities and mitigations.		☑					☑	☑			☑			
Assess culture & individual responsibilities.										☑				
Undertake ethical system reconnaissance and intelligence analysis.		☑			☑			☑						
Undertake risk modelling, analysis and trades.		☑			☑									☑
Undertake risk assessment to an external standard.	☑										☑			
Apply a management system and develop an information security management plan.	☑							☑			☑			
Configure and use security technology components and key management.	☑	☑								☑	☑			
Design & evaluate a system to a security case.	☑						☑			☑	☑	☑		
Architect, analyse & justify a secure system.	☑	☑								☑	☑			
Develop an assurance strategy.		☑						☑			☑	☑		
Security monitoring, analysis and intrusion detection. Recognise anomalies & behaviours.	☑							☑			☑			
Manage intrusion response, including with 3rd parties.	☑							☑			☑			
Organise testing & investigation work in accordance with legal & ethical requirements.		☑						☑		☑				

Modules/ Underpinning professional, interpersonal and business skills	Networks	Principles of Cyber Security	Principles of Databases	Principles of Programming	Professional Development	Web and Apps	Linux and Scripting	Computer Forensics	Employability Skills	Ethics and Ethical Hacking	Securing Networks	Project
Develop & apply information security policy to implement legal or regulatory requirements.					?				?	?		?
Fluent in written communications and able to articulate complex issues.					?							?
Makes concise, engaging and well-structured verbal presentations, arguments and explanations.					?				?			
Able to deal with different, competing interests within and outside the organisation with excellent negotiation skills.								?	?	?		?
Able to identify the preferences, motivations, strengths and limitations of other people and apply these insights to work more effectively with and to motivate others.					?				?			?
Able to work effectively with others to achieve a common goal.									?			?
Competent in active listening and in leading, influencing and persuading others.					?				?			
Able to give and receive feedback constructively and incorporate it into his/her own development and life-long learning.					?				?			?

Modules/ Behaviours	Networks	Principles of Cyber Security	Principles of Databases	Principles of Programming	Professional Development	Web and Apps	Linux and Scripting	Computer Forensics	Employability Skills	Ethics and Ethical Hacking	Securing Networks	Project
Analytical and critical thinking skills for Technology Solutions development and can systematically analyse and apply structured problem solving techniques to complex systems and situations.					?				?			?
Able to put forward, demonstrate value and gain commitment to a moderately complex technology-oriented solution, demonstrating understanding of business need, using open questions and summarising skills and basic negotiating skills.		?		?			?				?	
Can conduct effective research, using literature and other media.					?							?
Logical thinking and creative approach to problem solving.	?										?	
Able to demonstrate a 'security mind-set' (how to break as well as make).		?						?				
Demonstrates business disciplines, ethics and courtesies, demonstrating timeliness and focus when faced with distractions and the ability to complete tasks to a deadline with high quality.									?	?		?
Flexible attitude and ability to perform under pressure.								?	?			?

A thorough approach to work in the cyber security role	?	?			?		?	?	?	?	?	?