LEEDS BECKETT UNIVERSITY

Course Specification

BSc (Hons) Cyber Security and Digital Forensics

Course Code: BCSDF

2026/27

leedsbeckett.ac.uk

BSc (Hons) Cyber Security and Digital Forensics (BCSDF)

Applicant Facing Course Specification for 2026/27 Undergraduate Entrants

Confirmed at

General Information

Award	Bachelor of Science with Honours Cyber Security and Digital Forensics If you opt to undertake a full year placement and this is completed successfully you will have the words 'with placement year' added to the award title including for any contained awards that you are eligible for.
Contained Awards	Bachelor of Science Cyber Security and Digital Forensics (Level 6) Diploma of Higher Education Cyber Security and Digital Forensics (Level 5) Certificate of Higher Education Cyber Security and Digital Forensics (Level 4)
Awarding Body	Leeds Beckett University
Level of Qualification and Credits	Level 6 of the Framework for Higher Education Qualifications, with 120 credit points at each of Levels 4, 5 and 6 of the UK Credit Framework for Higher Education (360 credits in total). If you have opted to undertake a full year placement and complete this successfully you will achieve an additional 120 credit points at level 5. This will be included in your transcript.
Course Lengths and Standard Timescales	Start dates will be notified to students via their offer letter. The length and mode of delivery of the course is confirmed below: • 3 years (full time, campus based) • 4 years (full time, campus based, with placement year – if applicable)
Location(s) of Delivery	The majority of teaching will be at Headingley campus but on occasion may be at City campus Placement location, if applicable, will vary dependant on the opportunity.

Entry Requirements	Admissions criteria are confirmed in your offer letter. Details of how the University recognises prior learning and supports credit transfer are located here: https://www.leedsbeckett.ac.uk/student-information/course-information/recognition-of-prior-learning/ Admissions enquiries may be directed to: AdmissionsEnquiries@leedsbeckett.ac.uk.
Course Fees	Course fees are confirmed in your offer letter. A breakdown of any additional costs is included on the online prospectus entry for this course. Fees enquiries may be directed to Fees@leedsbeckett.ac.uk.

Policies, Standards and Regulations (https://www.leedsbeckett.ac.uk/our-university/public-information/academic-regulations/)

There are no additional or non-standard regulations which relate to your course.

Professional Accreditation or Recognition Associated with the Course

Professional Body

British Computer Society (BCS) – The Chartered Institute for IT

Accreditation/ Recognition Summary

A graduate meets some or all of the educational requirements for registration with BCS as a Chartered IT Professional (CITP). BCS will not accredit until graduates have exited the award.

Placement Information

Summary

The course contains a placement year.

Leeds Beckett is dedicated to improving the employability of our students and one of the ways in which we do this is to support our students to gain valuable work experience through work-based placements. Our placement teams have developed strong links with companies, many of whom repeatedly recruit our students into excellent placement roles and the teams are dedicated to supporting students through every stage of the placement process. More information about the many benefits of undertaking a work placement, along with details about how to contact our placement teams can be found here: http://www.leedsbeckett.ac.uk/studenthub/placement-information/

Placement Delivery

Students are responsible for obtaining their own placement, with assistance from the University.

Location

Placement location will vary dependant on the opportunity.

Approval

Whilst students source their own placements, they will need to meet requirements which will be outlined before module enrolment.

Other 'In Year' Work Placement Information

Summary

Work placement or volunteering opportunities may be supported throughout study at the University, informally.

Length

Varied as appropriate for opportunity

Location

The location may vary, dependent on the opportunity.

Timetable Information

Timetables for Semester 1 will be made available to students during induction week via:

i) The Student Portal (MyBeckett)
ii) The Leeds Beckett app

Any difficulties relating to timetabled sessions may be discussed with your Course Administrator.

Key Contacts

Your Course Director	Dr Pip Trevorrow
Your Course Administrator	Claire Howson - C.Howson@leedsbeckett.ac.uk

Course Overview

Aims

This course aims to bring together a merge of the disciplines cyber security and digital forensics. Students who undertake the course will be proficient within the two subject areas, and be in a position to perform digital forensic analysis and/or implement cyber security mechanisms into any business they obtain employment with.

With an increase in the use of digital devices within every walk of life this means that there is not a single crime that a digital device cannot be linked to. There is an ever growing demand for digital forensic techniques as the number of digital devices and the volume of data that can be stored rapidly increases. Cyber attacks are rising: the impact on companies both in terms of the financial implications and security breaches is significant and of concern. Companies and institutions are bound by the General Data Protection Regulation (GDPR), which requires that data be kept secure and accurate. Companies and institutions are only too aware of the legal implications of security breaches and leaked data and are therefore implementing more rigid and pronounced cyber security and management policies.

With the ever increasing use of digital devices and the risks posed by them, and an increase in recent years of cybercrime, it is commonly understood that the skill sets required for cyber security and digital forensics are essentially the same, and are complementary where they differ (or any differences are complementary). Students with the dual skill set are not only ultimately in the position to undertake a more rigorous digital forensic analysis, but also to implement more robust security mechanisms. Fundamental to this is the understanding of computer systems and the broader computing field which is addressed throughout the levels of the course.

Students on the Cyber Security and Digital Forensics course will learn to not only secure and test the security of computer systems and networks, but will also be able to analyse the systems for evidence of breaches following evidential standards. Students will learn through practical applications on our bespoke Hacktivity system designed and created, in house, to replicate real world business systems and potential attacks. Students will gain expertise in the use of digital forensic techniques and analysis through appropriate tools, commercially used in industry (Encase, Cellebrite) and open source variants (Autopsy, FTK Imager), and will develop an understanding of the motivation for crimes. Students will also work with employers, lawyers and experts to gain experience of preparing work for use by courts and customers and subsequently presenting it.

The two subject areas have many facets, and therefore the numbers of optional modules within the award are limited. This allows the teaching team to cover the two subject areas to the depth expected of a graduate with such a degree.

The programme will provide a mix of academic and practical content; provide students with the theoretical knowledge to excel in their field and the practical experience to be able to physically implement their skills. The course will allow students who are unsure as to which field to focus on, to become proficient in both; creating additional career paths.

The course aims to prepare students for a career in the cyber security and/or digital forensics industry working with small consultancies or large organisations, including the police. However, the course will also prepare students for any career in the IT sector including software development, web design, IT network management and database administration within business, voluntary or public sectors.

Course Learning Outcomes

At the end of the course, students will be able to:

1	A systematic understanding of key aspects of cyber security and digital forensics, including acquisition of coherent and detailed knowledge, at least some of which is at, or informed by, the forefront of the discipline.
2	An ability to deploy accurately established techniques of analysis and design that encompass internationally recognised standards.
3	A wide breadth of understanding that enables students to devise and sustain arguments and solve problems using ideas and techniques, some of which are at the forefront of cyber security and digital forensics practice, and describe and comment upon particular aspects of current research, or equivalent advanced scholarship.
4	The skills and understanding to undertake projects to a professional industry recognised standard, within cyber security and digital forensics, by the consistent application and review of development, management and evaluation methods and techniques.
5	An ability to independently undertake research and critically evaluate arguments, assumptions, abstract concepts and data (that may be incomplete), to make judgements, and to frame appropriate questions to achieve a solution or identify a range of solutions to a problem.
6	A detailed and critical understanding of the legal, social, ethical and professional issues pertaining to cyber security and digital forensics and which have a significant influence on professional practice in these fields.

Teaching and Learning Activities

Summary

For each module students will normally receive a weekly lecture followed by a tutorial or practical lab based session(s). In addition, some modules will be supplemented with optional drop-in workshop sessions. These are supplemented with a programme of guest speakers and/or industry led seminars. This structure is preferred within such a vocational award where students are learning specialised material for a specific career.

This is a very hands-on subject area where theory alone would be unlikely to allow a student to achieve successful employment in this area. Practical exercises allow for students to implement their theoretical learning and see how it relates to industry. Practical solutions are achieved through the replication of exercises such as compromised computer systems and mobile devices that students must analyse – similar to that as found in industry. Many of these examples are available through open source community projects but are also built in-house when suitable external material is not available.

The use of a team project at Level 5 allows students to develop communication skills with their peers, this will include where possible, mixing with other cultures and individuals that they may not have originally chosen to work with as they are outside of their direct friendship group. Any issues that arise within group work such as difficulties with other group members are carefully managed through distanced support of the group where possible, to encourage the students to deal with the issues themselves. Where distance support is not possible tutors will directly resolve the issue working with the group to rectify and identify solutions.

Students are encouraged to debate within a variety of learning environments, including in-class and through the VLE discussion boards and additional chat applications where appropriate – this helps to develop respectful appreciation of their peers. Through encouraging students to use industry forums and scholarly research, students interact with a range of cultures and thinking that they are required to draw upon and evaluate within several modules.

The use of an induction session begins the process of welcoming students to the University and the course. Students are introduced to the support mechanisms in place, school and university wide, and begin to develop relationships with their peers. Students are placed into small teaching /tutorial groups that they will remain with for the first year of their study. Each group has an assigned Academic Adviser who will run weekly Course Tutorials (external to the formal teaching modules) with their group during each semester. The Course Tutorials cover elements such as academic integrity, study plans, referencing, employability; in order to help support the students learning and progression through their first year of study. Each student will have a one to one meeting with their Academic Adviser at least once a semester in order to discuss progress and help with settling into university life.

This course will feature a mix of blended learning, both online and in-person. Lectures will be a mix of recorded and live. Tutorial/Seminar sessions will all be in-person as per the timetable.

Your Modules

This information is correct for students progressing through the programme within standard timescales. Option modules listed are indicative of a typical year. There may be some variance in the availability of option modules. Students who are required to undertake repeat study may be taught alternate modules which meet the overall course learning outcomes. Details of module delivery will be provided in your timetable.

Level 4
Compulsory modules

Module title	**Credits**	**Semester/ teaching period**
Fundamentals of Digital Forensics	20	S1
Computer Communications	20	S1
Fundamentals of Computer Programming	20	S1
Ethical Hacking and Penetration Testing	20	S2
Fundamentals of Databases	20	S2
Object Oriented Programming	20	S2
Number of credits of compulsory modules	120	

Level 5
Compulsory modules

Module title	Credits	Semester/ teaching period
Digital Forensic Processing	20	S1
Cyber Security Landscapes	20	S1
Web and Network Security	20	S2
Digital Forensics Analysis	20	S2
Team Project	20	S2
Number of credits of compulsory modules	100	

Option modules

Module title	Credits	Semester/ teaching period
Database Systems	20	S1
Web Application and Technologies	20	S1
Software Systems Development	20	S1
Number of credits of option modules a student should choose	20	

Placement year (if chosen) – Core Module

Module title	Credits	Semester/ teaching period
Placement Module	120	Min 40 weeks

Level 6
Compulsory modules

Module title	Credits	Semester/ teaching period
Production Project	40	S1 & S2
Mobile Forensics Investigation	20	S2
Systems Security	20	S2
Number of credits of compulsory modules	80	

Option modules

Module title	Credits	Semester/ teaching period
Forensic Investigative Techniques	20	S1
Incident Response and Investigation	20	S1
Advanced Database Systems	20	S1
Advanced Web Engineering	20	S1
Advanced Software Engineering	20	S1
Number of credits of option modules a student should choose	40	

Assessment Balance and Scheduled Learning and Teaching Activities by Level

The assessment balance and overall workload associated with this course are calculated from core modules and typical option module choices undertaken by students on the course. They have been reviewed and confirmed as representative by the Course Director but applicants should note that the specific option choices students make may influence both assessment and workload balance.

A standard module equates to 200 notional learning hours, which may be comprised of teaching, learning and assessment, any embedded placement activities and independent study. Modules may have more than one component of assessment.

Assessment

Level 4 is assessed by coursework and practical assessments

Level 5 is assessed by coursework and practical assessments

Level 5 placement is assessed by presentation and a report

Level 6 is assessed by coursework and practical assessments

Workload

Overall Workload	**Level 4**	**Level 5**	**Level 5 placement (if chosen)**	**Level 6**
Teaching, Learning and Assessment	270 hours	219 hours		171 hours
Independent Study	930 hours	981 hours		1029 hours
Placement			1400 hours	