Introduction and special features
Our MSc in Cyber Security offers a highly dynamic, student focused study and delivery model that empowers you as a learner and facilitates your professional development and learning needs in the midst of a rapidly changing and demanding world.

A Different Kind of Master’s Provision
This part-time only Master’s programme has been designed for professionals seeking to either transfer into, or progress further, in the field of cyber-security. We have worked closely with contacts in industry and in the public sector to produce a tightly written professionally informed programme that will recruit predominantly students who are currently in full time highly specialised roles. Although some students may self-fund it is envisioned that many students on the programme will be funded by their employers. Due to these factors this programme will be structured, delivered, costed and marketed in a way that is very different to many other master’s programmes. In some ways this has much in common with executive education.

Lego Brick Structure
The modular structure is designed in a ‘Lego brick’ model. The modules can be taken in any order, there are no pre-requisites. Therefore, like Lego bricks, these can be assembled in any available way to create the MSc module profile you wish. As a student, you will be given an academic supervisor who can offer advice on which modules may suit your aspirations, but you are able to structure your learning to suit your current employment context, knowledge, skills and learning pace. For example, if you are a strong programmer but weak at networking you may wish to study secure programming early on in MSc studies, while committing to self-study in your personal time to prepare you to undertake the secure networking module, later on in your studies, when you feel your skills are adequate to enable you to do so.

The Modules
All of the modules on this programme have both a distance learning element and an immersive element. You are sent preparation materials approximately six working weeks before a module’s due start date. You then engage in self-study of this material in preparation for a week
of on-site immersive education at York St John University. On the week of taught delivery, you will come to York St John for intensive and immersive classes that run from Monday to Friday, typically 09:00 to 17:00. In these classes you will build on the pre-study material, consolidating your learning through practical and theoretical learning experiences. On the last day of this class, you will leave with an assignment, which must be completed within six to eight weeks, depending on the module focus.

The programme provides you as an aspiring MSc student with a fantastic opportunity to upgrade your skills-set and expand your professional network through working with other people with a shared professional focus on cyber-security. It also allows you to acquire highly sought-after specialist skills one Lego brick at a time.

If you are seeking to complete this programme within a three-year time frame you should take three to four modules per year and begin your major project module when you have completed approximately five modules.

**Admissions criteria**

You must meet the University’s general entry criteria for postgraduate study. In addition, you must have:

- **Either:**
  - An existing undergraduate degree in a related field, such as computer science or software engineering, or;
  - Professional experience that demonstrates a propensity for studying cyber security. For example, you may be or have been a member of the police or other services. You may work in a system administrator's role and have several professional qualifications, but lack academic ones, or;
  - Clear and demonstrable technical abilities in the field of computing that would have equivalency to that of an individual who has completed a degree in a related field, or;
  - Clear and demonstrable skills in the field of law and/or policy with postgraduate level research skills and some training skills, with a self-motivated approach to acquiring more through independent studies to enable you to undertake the technical aspects of this programme of study, or;
  - Where appropriate, candidates will be interviewed to ensure that they are suitable for the programme.

If your first language is not English, you need to take an IELTS test or an equivalent qualification accepted by the University (see [https://www.yorksj.ac.uk/international/how-to-apply/english-language-requirements/](https://www.yorksj.ac.uk/international/how-to-apply/english-language-requirements/)).

If you do not have traditional qualifications, you may be eligible for entry on the basis of Accredited Prior (Experiential) Learning (APL/APEL). We also consider applications for entry with advanced standing.

**Programme aims**

This programme aims to develop graduates with the necessary technical and higher-level reasoning skills required of a cyber-security professional. The programme does this through a learning-through-doing approach, which offers multiple opportunities to learn practical skills and conceptual techniques from specialist areas in cyber-security. This equips students with the technical knowledge, analytical abilities and organisational methods to propose, research, develop and complete a self-directed research project.

Students work with simulations of real world scenarios to develop higher level reasoning skills and prepare them for complex work in cyber-security. This enables them to understand the practical, professional and ethical skills demanded by industry, and to develop a critical, analytical, systematic and comprehensive understanding of the field of cyber-security.
Programme learning outcomes

Upon successful completion of the programme you will be able to:

Level 7

7.1 Apply tools and technical skills to identify, model, and critically evaluate cyber-security threats.

7.2 Use established concepts and techniques from the study of cyber-security to propose and analyse solutions to a range of cyber-security challenges.

7.3 Solve a range of current and emerging cyber-security problems, demonstrating a systematic understanding and application of appropriate security tools and techniques.

7.4 Demonstrate compliance with the laws governing the field of cyber-security and create policies for addressing cyber-security threats.

7.5 Evaluate, refine, and apply comprehensive analytical and technical skills to solving a significant cyber-security challenge.

7.6 Define a problem, and professionally manage a process of work to propose and execute a viable and ethical solution to it, relevant to the field of study, using a project management methodology.

Programme Structure

<table>
<thead>
<tr>
<th>Code</th>
<th>Level</th>
<th>Title</th>
<th>Credits</th>
<th>Status of Module*</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSY001</td>
<td>7</td>
<td>Security Fundamentals</td>
<td>10</td>
<td>O</td>
</tr>
<tr>
<td>MSY002</td>
<td>7</td>
<td>Risk Management and Response</td>
<td>10</td>
<td>O</td>
</tr>
<tr>
<td>MSY003</td>
<td>7</td>
<td>Policy and Governance</td>
<td>10</td>
<td>O</td>
</tr>
<tr>
<td>MSY004</td>
<td>7</td>
<td>Secure Design</td>
<td>10</td>
<td>O</td>
</tr>
<tr>
<td>MSY005</td>
<td>7</td>
<td>Social Engineering</td>
<td>10</td>
<td>O</td>
</tr>
<tr>
<td>MSY006</td>
<td>7</td>
<td>Data Security</td>
<td>10</td>
<td>O</td>
</tr>
<tr>
<td>MSY007</td>
<td>7</td>
<td>Network Security</td>
<td>10</td>
<td>O</td>
</tr>
<tr>
<td>MSY008</td>
<td>7</td>
<td>Forensics</td>
<td>10</td>
<td>O</td>
</tr>
<tr>
<td>MSY009</td>
<td>7</td>
<td>Secure Programming</td>
<td>10</td>
<td>O</td>
</tr>
<tr>
<td>MSY010</td>
<td>7</td>
<td>Wireless Networks security</td>
<td>10</td>
<td>O</td>
</tr>
<tr>
<td>MSY011</td>
<td>7</td>
<td>Reverse Engineering</td>
<td>10</td>
<td>O</td>
</tr>
<tr>
<td>MSY012</td>
<td>7</td>
<td>Research Methods</td>
<td>20</td>
<td>CA</td>
</tr>
<tr>
<td>MSY013</td>
<td>7</td>
<td>Major Project</td>
<td>60</td>
<td>CA</td>
</tr>
</tbody>
</table>

*C: Compulsory, CA: Compulsory for award, O: option or E: elective.

Learning, teaching and assessment

The teaching, learning and assessment philosophy underpinning this programme is derived from the recognition that while information may be all around us, knowledge is something we hold within ourselves. Further, that information becomes knowledge through its application to solving challenges. Thus throughout your studies you will be encouraged to apply your knowledge and so learn through doing.

At the start of your MSc you will be assigned a supervisor. The Supervisor will be your main mentor and point of contact for the duration of your studies. You will be able to book tutorials
with them and seek guidance with regards the development and progression of your study. Typically upon starting your MSc programme, you are expected to arrange an initial meeting with your supervisor in which you present and discuss your plans for managing your MSc studies, including your module choices. Your supervisor will be able to discuss these with you and offer other academic advice to help you manage your study.

Each module exposes you to focused study of information within a discrete area of cyber-security. This begins through your engagement with pre-study material. Then, through a week of immersive education, you are exposed to further information and encouraged to apply it in order to solve challenges of varying difficulty. This will be done through the application of a range of teaching and learning techniques, helping you explore the information, testing and applying it so that it starts to become internalised as knowledge.

You are then challenged to apply your developing knowledge further through the module assignment. The assignment draws upon what you have learned in class and requires you to apply it to further challenges that are reflective of real world scenarios. Assessments typically take the form of an artefact based project which includes practical and theoretical assessment challenges requiring you to apply and test the material covered during your module. As modules vary greatly, so too do the content of the artefact. Thus the assessment process encourages you to consolidate your learning throughout the module.

Each module takes the above approach so that by the end of your studies you have built a body of practical and conceptual knowledge affording you a range of developing professional competencies. Formative assessment will be employed throughout the programme through a range of tasks, projects and presentations. Summative assessment will take a variety of forms reflective of the kinds of demands placed upon you in a professional environment. These may include written reports, case studies, policy document development and practical software engineering processes and evaluations.

The major project challenges you to apply all of your learning to date in identifying and solving a non-trivial cyber-security challenge. It enables you, in discussion with your supervisor, to design a research project to best show case your skills and interests, as well as provide a challenge to consolidate your learning to date at a level appropriate for the award of an MSc in Cyber Security.

The programme has been designed to meet the needs of both students who have just finished undergraduate programmes in the UK/EU and International and returners to learning.

Please note that all modules are subject to staffing and timetable availability each year.

**Progression and graduation requirements**
The University’s [general regulations for](#) postgraduate awards apply to this programme.

Any modules that must be passed for progression or award are indicated in the Programme Structure section.

**Internal and external reference points**
This programme specification was formulated with reference to:

- University Mission Statement [see page two]
- Strategic Plan 2015-20 [see page four]
- QAA subject benchmark statement
- Framework for Higher Education Qualifications

*Date written / revised:*

*Programme originally approved:*