



Proposal for MSc in Cyber Security, Privacy, and Trust (Graduate-Level Apprenticeship) Stage 1

Contents

1 OVERVIEW OF PROGRAMME

ABOUT THE PROGRAMME

2 BUSINESS CASE

STRATEGIC PLANNING, RECRUITMENT & COMPETITOR ANALYSIS

FEES AND COSTING

ANTICIPATED AND PROJECTED ENROLMENTS

PLANNING AND RESOURCES

COLLABORATIVE PROGRAMMES

3 CONSULTATION AND APPROVAL

STAGE 1: CONSULTATION

STAGE 2: SCHOOL BOARD OF STUDIES REVIEW AND APPROVAL

STAGE 3: HEAD OF SCHOOL REVIEW AND APPROVAL

STAGE 4: COLLEGE CURRICULUM APPROVAL BOARD REVIEW AND OUTCOME

OVERVIEW OF PROGRAMME

Grey text has been added to provide guidance. Please delete as you add your own text, remove italics, and change the font colour to black.

ABOUT THE PROGRAMME		
Title of programme	<i>Cyber Security, Privacy, and Trust (Graduate-Level Apprenticeship)</i>	
Intended Award	MSc	
Alternative awards	<i>(Insert name e.g. PG Dip, PG Cert)</i>	
School	School of Informatics	
Programme Director		
Programme start dates	2019-2020	
SCQF level of highest award		
Total credit value of programme <i>(for highest award)</i>	180	
Partner institution(s) if any	Because it is a Graduate-Level Apprenticeship it will be delivered in partnership with collaborating employers.	
Mode of delivery <i>(Please ✓ those which apply to this programme)</i>	On campus	Y
	Online	Y
	Blended learning	Y
	FT	Y
	PT	Y
	Intermittent	N
Expected length of programme	FT	N
	PT	24 months
	Intermittent	N
Description of the programme and its structure (maximum 150 words)		
The graduate apprenticeship variant of the MSc in Cyber Security, Privacy, and Trust programme is a response to the growing need for highly specialised training in this area and which provides students with the skills to analyse cyber security to inform their employer organisation's cyber security resilience activities. The graduate apprenticeship aligns to the Skills		

Development Scotland (SDS) published Graduate Apprenticeship SCQF level 11 framework in Cyber Security. It also supports the Scottish Government Learning & Skills Action Plan for Cyber Security Resilience 2018-2020.

The course is a graduate apprenticeship so students will cover academic material at University and the application of that material in workplace-based learning working for their employer. This is a roughly equal blend of workplace and academic setting. As an apprentice, students will be employed and paid a salary by their employer and will be treated as normal employees of the company under their usual terms and conditions. Students will likely either be existing employees of the firm or new graduate hires. In either case they will be seeking to develop their cyber security knowledge and skills through this GA programme with the benefit of an employer context to relate these to.

The increasing reliance of services on information technology in both the public and private sector has raised significantly the potential impact for cyberattacks in the last two decades. In 2016 alone the impact on global economy was as high as \$450 Billion, according to reports from Hiscox and others, while the cyber security threat has been characterised as serious as terrorism by the GCHQ. At the same time, industry research firms like Gartner measure the current size of cyber security industry as \$86 Billion and various predictions of growth in the next 5 years estimate that the size of the industry will double at minimum. Despite the dire need for highly qualified personnel, the industry is facing a serious shortage and there are projections of more than 1.5 million unfilled positions by 2020. The above facts paint a picture that demands immediate action from universities to provide the vision and necessary training for the security experts that can meet the challenge of securing information technology services in the next five to ten years.

Training at the postgraduate level can be an extremely effective catalyst given the lack of systematised secure engineering practices in information technology and the rapidly evolving nature of information technology services. The programme will aim to create a generation of leaders in the security and privacy sectors (both in academia and industry).

The security and privacy group at the School of Informatics conducts research on all aspects of the core technology and applications. The proposed specialism courses cover fundamental topics: Secure Software, Cryptography, Secure Hardware, Verification, Post Quantum, Data Privacy, Usability, Fintech, Health, Smart Contracts, Distributed Ledgers, Privacy Preserving Data Mining. The teaching team of the MSc in Cyber Security, Privacy, and Trust is lined up with world class researchers and educators. In particular, the University has been recognised by GCHQ/NCSC as an Academic Centre of Excellence in Cyber Security Research, in recognition of its critical mass in leading edge cyber security research.

The curriculum is designed in such a way (see proposed DPT of the Programme), that each GA student will receive a tailor-made training regime that is suitable for their focal area and employment within cyber security and privacy, but will also develop a joint perspective on cyber security.

Career, employability and opportunities for continuing professional development.

The graduates will have the necessary background to keep up with developments in cyber security, both in research and engineering. Typical areas to pursue a career include: Security Analyst, Security Architect, Security Engineer, Security Administrator, Cyber Risk Analyst, Cryptographer, Cryptanalyst, Security Consultant, Security Auditor, Secure Software Developer, Penetration Tester, Ethical Hacker, Security Researcher (in academia or industry), as well as security officers of various kinds in government and public sector positions (the National Cyber Security Centre has explicitly expressed interest in collaborating with our program). There are well established career development paths and certification schemes including CISSP (Certified Information Systems Security Professional) run by ISC2 ([International Information System Security Certification Consortium](https://www.isc2.org/)). There is a new UK government-sponsored initiative delivering a new Cyber Security Body of Knowledge (<https://www.cybok.org/>) which is intended to describe curricula frameworks for the future, to inform and underpin education and professional training for the cyber security sector.

“There is zero percent unemployment in cyber security and opportunities are endless” says Herjavec from Cybersecurity Ventures.

Employers will recruit new graduate hires with relevant degree level qualifications. There is a serious global shortage of Cyber Security professionals and the combination of strong academic training and practical experience will make graduates of the programme highly employable and of increased value to their employers.

BUSINESS CASE

Cyber Security is currently the only graduate apprenticeship programme supported by Skills Development Scotland at level 11. It responds to the strategic need to develop Cyber Security resilience skills in Scotland. The Learning & Skills Action Plan for Cyber Security Resilience 2018-2020 published by the Scottish Government in March 2018 aims to:

- Explicitly embed cyber resilience throughout our education and lifelong learning system
- Increase people's cyber resilience at work
- Develop the cyber security workforce and profession to ensure that skills supply meets demand and that skilled individuals can find rewarding employment in Scotland.

The proposed graduate apprenticeship supports these aims as well as pointing to wider benefit to the University developing such provision and new collaborations with employers.

The original employer technical expert group (TEG) included the following public and private employer organisations who were all focussed on the strategic need develop new university led initiatives to develop higher level skills through relevant academic provision and leading to recognised MSc qualifications.

- Scottish Government
- BBC
- BT
- DXC
- Lloyds Banking Group
- Morgan Stanley
- NHS
- Police Scotland
- Tesco Bank

Already several of the above employers have committed to using the GA in Cyber Security, Privacy and Trust at the University of Edinburgh, with several more keen to support using the programme in the future.


This is not a conventional business case. The programme is seen as strategically useful since it positions the University as a key high-quality skills provider in the context of the Cyber Security Skills agenda in Scotland, and supports to need to develop increased employer collaboration as part of the GCHQ Centre of Excellence for Cyber Security Research.

STRATEGIC PLANNING, RECRUITMENT & COMPETITOR ANALYSIS	
Programme Title	MSc in Cyber Security, Privacy, and Trust
Programme Proposer	Myrto Arapinis, David Aspinall, Elham Kashefi, Aggelos Kiayias, Markulf Kohlweiss, Kami Vaniea, Petros Wallden, and Vassilis Zikas
Strategic Planning	<p>Graduate Level Apprenticeships are seen as a key element in the Scottish Skills Strategy and the Learning & Skills Action Plan for Cyber Security Resilience 2018-2020. This programme is an early “experiment” to see what is required to deliver in this mode and to explore the relationship with Scottish Government in Cyber Security Skills provision.</p> <p>Cyber Security and privacy present challenges to nation and society. The solutions will involve science and engineering, as well as people and politics. Our proposed new MSc programme has been on the Informatics School Plan since Cyber Security was targeted as a growth area in 2012/13.</p> <p>The MSc is part of a wider initiative across the University to establish a network of researchers and forms a stage in connecting relevant courses across multiple disciplines. It fits with the University's Data Driven Innovation strategy and its Secure Data Storage strand, which we expect must evolve to encompass research more broadly on Cyber Security and Privacy, concerning information (data in context) and building a new science of trust and identity.</p> <p>The University has been exploring opportunities related to the Apprenticeship Levy; Cyber Security is one of the demand areas for Graduate Apprenticeships which is scheduled for future development for MSc and online programmes (Apprenticeship update April 2018).</p>
Recruitment <i>Please provide a detailed commentary on your marketing and recruitment strategy.</i>	<p>Our goal is to recruit a small cohort of companies that are prepared to sponsor students who will be from their existing workforce. We have already secured 3 large and diverse companies who have given their commitment to use the programme. These are Scottish Government Cyber Security Resilience Team, Tesco bank and Morgan Stanley. Student numbers will be 10 in the first year, then increasing to 25 or more thereafter.</p> <p>There is a strong push from central government for research and teaching in cyber security, as part of the national UK Cyber Security Strategy. This is because there is a dire need for highly qualified personnel. The industry is facing a serious shortage in the area, and there are projections of more than 1.5 million unfilled positions by 2020.</p> <p>The programme targets students who already are, or who aspire to become cyber security professionals in the cyber security and privacy space. Top graduates of the programme will follow careers leading to high-profile positions such as Chief Information Security Officer (leader of all security initiatives in a company), Security Consultants (design the best possible security solutions), Security Architects (design, build, and oversee the implementation of network and computer security for a company), as well as Computer Forensics experts (responsible for conducting security incident investigations), Penetration Testers (responsible for legally hacking into an organization’s applications), Security Analysts (responsible for detecting and preventing cyberthreats for a company), Security Software Developers (responsible for integrating security into applications software during the design and development process), Security Auditors (mid-level role responsible for examining the safety and effectiveness of company computer systems and their security components).</p>

	<p>Developing new relationships with employers using the graduate apprenticeship opens up the potential for increased research collaboration and also offers direct career routes for current masters and research students to develop careers as cyber security professionals. Besides the usual marketing channels that employers, the School and University might employ to attract the graduate hires to undertake the GA programme, there is obvious attractiveness to Informatics graduates coming to the end of their degree programmes as well as students across the Edinburgh region. There are a number of channels that can be used for recruiting for and marketing the MSc in Cyber Security, Privacy, and Trust:</p> <ul style="list-style-type: none"> • The School of Informatics hosts each year the Cyber Security Christmas lectures, which are attended by around 600 high school pupils. These are highly publicised events putting us on the map as a leading University in cyber security teaching. • Our undergraduate students have had prominent recent successes in Cyber Security Competitions including the recent ACE-CSR UK University's competition in Cambridge. One of our undergraduate students having won the C2C competition this year. These set up the University as one of the leading universities in security teaching, and increase our visibility towards prospective students interested in security, but also towards industry and public sector organisations. This can in turn open funding and employment opportunities for our students. <p>Furthermore, the National Cyber Security Centre (NCSC) and its government partners have initiated across UK academia a degree certification programme to address the knowledge, skills and capability requirements for cyber security research and education. The vision of the UK Cyber Security Strategy 2016-21 is that: "the UK is secure and resilient to cyber threats, prosperous and confident in the digital world." And Section 7 of the Strategy ('Develop') states that: "the UK requires more talented and qualified cyber security professionals". In particular, objective 7.1 is "to ensure the sustained supply of the best possible home-grown cyber security talent". The curriculum is carefully designed with the intention to obtain this certification by the NCSC. NCSC-certification will help us attract high quality students from around the world. It will also help employers recruit skilled staff, and guide prospective students in making better informed choices when looking for a highly valued qualification.</p> <p>This programme should not directly impact any other of our programmes. This is a specialised MSc programme that does not overlap with the other specialised MSc programmes such as the MSc in Data Science, MSc in Cognitive Science or MSc in Artificial Intelligence in their core courses. Students enrolled in our MSc in Computer Science and MSc in Informatics can currently follow the Cyber Security and Privacy area. These students might decide to enrol in a programme formally branded as such. The new courses that will be introduced will also be available for our undergraduate students, enhancing their experience with more choice in the area of cyber security, privacy, and trust. This might particularly be attractive to our Minf students.</p>
<p>Competitor Analysis <i>A competitor analysis report provides a better understanding of the marketplace and competition, from the going rate for tuition fees to the unique selling points and</i></p>	<p>The main competitors for the GA in Cyber Security are likely to be The University of Strathclyde, Glasgow University and Edinburgh Napier and Abertay Universities.</p> <p>Our proposed MSc covers a wide range of topics, ranging from modern cryptography to usable security and cybercrime and will be of particular and distinctive appeal to employers. We have a very strong Security and Privacy research group (10 academics) and in 2017 we obtained recognition as Academic Centre of Excellence for Cyber Security Research (ACE-CSR) by the National Cyber Security Centre (NCSC),</p>

<p><i>marketing strategies of competitor programmes.</i></p>	<p>being the first (and only) Scottish University having achieved this. This strengthens our course by offering the opportunity to students to be taught a wide range of topics from leading experts in each particular area. Moreover, we offer a number of highly specialised courses, such as “Blockchains and Distributed Ledgers”, “Cryptanalysis” and “Quantum Cyber Security”, that are likely to attract ambitious students and distinguish us from our competitors. The structure of the course we offer is tailor-made to obtain NCSC certification and is similar with our leading competitors (for example the MSc in Cyber Security in Birmingham) that have already obtained such certification. As far as the local competition in Scotland is concerned, the Scottish Security MSc’s offered contain very different courses with different focus.</p>			
<p>Competitor Fees</p> <p><i>Provide the fee structure (in British pounds) of three competitors, preferably those mentioned in the competitor analysis. These may be UK or International competitors.</i></p>	<p>Institution</p>	<p>Programme</p>	<p>Fees</p>	
			<p>Home</p>	<p>International</p>
	<p>Edinburgh Napier University</p>	<p>MSc in Advanced Security and Digital Forensics (website)</p>	<p>£5,850</p>	<p>£15,150</p>
	<p>University of Glasgow</p>	<p>MSc in Information Security (website)</p>	<p>£7,650</p>	<p>£20,150</p>
<p>Abertay University</p>	<p>MSc Ethical Hacking and Cyber Security (website)</p>	<p>£5,500</p>	<p>£14,250</p>	

<p>FEES AND COSTING</p>		
<p>Programme fees</p> <p><i>Fees are expressed per academic year in British pounds. For PGT programmes, a Programme Costing Template will also be required for Fee Strategy Group.</i></p>	<p>Home-Scotland / EU</p>	<p>£14,774 Paid by Apprenticeships Scotland</p>
	<p>Home-RUK</p>	<p>£14,774 Paid by Apprenticeships Scotland</p>

	Overseas	n/a
<p>Fees for each new PGT programme are sent by College to the Fee Strategy Group (FSG) for review and approval. The FSG has developed a Programme Costing Template to give FSG insight into the anticipated profitability of a programme and where it sits within its market. The Fees Costings template, and guidance from FSG on filling out the template is included in the spreadsheet attached to the right.</p>		 FSGProgrammeCostingTemplate_03_01_19
Additional Programme Costs (PGR only)		
<p><i>Additional costs to the student should be noted and justified in the table below. These should consist of items that are over and above the basic provision that should be available to all students and should reflect the special additional costs associated with the specific programme of study. Individual items over £200 should be noted on a separate row.</i></p>		
Item	Cost	% of Total
No Additional Costs		
Total:	£0	100%

ANTICIPATED AND PROJECTED ENROLMENTS			
<i>What are the anticipated and projected enrolments over the next three years?</i>			
	Year 1	Year 2	Year 3
Home	10	15	20
International	0	0	0
Supporting Research What market research has been planned or completed to support the predicted student numbers?	<p>The year 1 numbers have been agreed between the University and Skills Development Scotland (who fund the graduate apprenticeships). Employers have agreed commitments that support the initial cohort. We anticipate a year on year rise in years two and three as more employers choose to support the programme.</p> <p>There is increasing demand for Cyber Security skills and qualifications and there is good demand from students through historical enrolment in the cyber security specialism, the number of students enrolled in cyber security courses, and students who ended up completing a security MSc project. Despite not being advertised at all, the current GA cyber security has attracted the full quota for the initial cohort.</p> <p>The school has a history of attracting students onto specialized MSc degrees such as the Masters in Design Informatics and the Masters in Artificial Intelligence, both of which regularly reach numbers similar or larger than the ones above. The University of Edinburgh was</p>		

	<p>also recently recognized as an Academic Centre of Excellence in Cyber Security Research by the UK National Cyber Security Center which has massively improved our visibility in Scotland and across the UK. The majority of other ACE-CSR Universities also run MSc programs in the area with similar intake numbers to the ones described above.</p> <p>It is anticipated that this MSc program will be able to run for an extended time period and be sustainable. Cyber Security is a cross-area problem impacting nearly all aspects of Computer Science and as a result, a good number of academic staff within the school work on it directly or indirectly. The most likely cause of sustainability issues for the program would be if we no longer have enough staff to teach the courses or take on project students. Given our current status as an ACE-CSR and the number of staff who work directly and indirectly on security issues, the risk of such a situation is low.</p>
--	--

PLANNING AND RESOURCES	
New Courses	<p>A new cyber security work based professional practice course will be introduced to complement the courses already taught. This will be in line with the work based professional practice courses already developed and approved for the GA in Data Science.</p> <p>The initial course proposal for the cyber security work based professional practice course will be submitted for approval by the Board of Studies. The Professional Practice course mirrors those already developed and approved as part of the graduate apprenticeship in Data Science. This will again be developed using the same approach and through the specialist expertise hired by the City Deal project.</p>
Facilities and Equipment	<p>The programme does not have extra estates requirements or equipment requirements besides access to the recently approved IoT and Cyber Security lab and the Cyber Security Research and Training lab based on the 5th floor of Appleton Tower. This graduate apprenticeship variant of the MSc in Cyber Security, Privacy and Trust has no additional requirements for facilities and equipment beyond those required for the full time programme and these students will benefit from their own employer contextualisation of cyber security technology, management and practice.</p> <p>Within the university to study and research practical network and software security, dedicated practical lab environments are essential. These two labs allow: network monitoring and data gathering under controlled conditions; isolated experiments with viruses, trojans, botnets and other kinds of malicious code; and practical hacking and penetration testing exercises. Students enrolled on the programme will have access when pertinent to the IoT and Cyber Security lab as well as the Cyber Security Research and Training lab. This will greatly enhance the students' experience, in particular during their summer projects. This will expose students to more hands-on security training and penetration-testing training.</p>
Staff	<p>The proposed DPT includes 7 specialist courses, 5 of which are already being resourced by the School of Informatics. The Security and Privacy group consists of 10 academic staff (2 joining early 2019) who will mainly teach the security related courses. So, there is in the School adequate teaching staff to resource the programme, but also to maintain the curriculum and introduce new courses if judged pertinent in the future. The group also includes more than 10 PhD students, many of them already supporting the security related teaching activities of the group.</p>

	<p>Given our current status as an ACE-CSR and the very substantial commitment the University has made in growing in terms of faculty with expertise in security and privacy, leading to 7 faculty hires at all academic levels during the past three years, the risk of not having adequate teaching staff for the core courses of the programme is low. If our CDT application is successful in this area this will significantly increase PhD numbers.</p> <p>It is likely that workplace-based courses will require specialist staffing. It is anticipated that a similar approach would be taken as for the GA in Data Science where a specialist university teacher role was recruited to support the GA in Data Science as personal tutor and work based tutor for the full cohort.</p>
Resource Sharing	<p>Given the scope of the proposed programme, the proposed DPT includes optional courses from the School of Law, the School of Social and Political Science, and the Deanery of Molecular, Genetic and Population Health Sciences (see attached case for support). All the course organisers of courses outside the School of Informatics and included in the DPT have been contacted and have welcomed the creation of such a focused programme with enthusiasm. They have given their consent for their courses to be included in the DPT of the MSc in Cyber Security, Privacy, and Trust.</p> <p>Some of the courses having restricted capacity, we will need to devise rules for prioritising students registration. This aspect has not yet been finalised and will be discussed in Autumn 2018. Such rules need to be devised carefully and require approval of the corresponding Board of Studies.</p> <p>This programme is effectively a means to boost the number of students on the MSc Cyber Security, Privacy and Trust, though the GA students will undertake the programme at 50% the rate of course / credits as the programme is developed over 2 years to align to the students employed roles with their employers.</p>

COLLABORATIVE PROGRAMMES	
<p>Additional information is required for new programmes that are collaborations with external institutions or organisations which will result in a joint award and/or where taught components are shared. International partnerships must have a Memorandum of Understanding (MoU) in place before the programme can be approved by College.</p> <p>Should the proposal be progressed to Stage 2 a draft Memorandum of Agreement (MoA) will need to accompany the submission.</p> <p>Separate guidance is available for the development of collaborative programmes.</p> <p>http://www.ed.ac.uk/governance-strategic-planning/collaborative-activity/guidance-templates</p>	
N/A	

CONSULTATION AND APPROVAL

Programme Title:	Cyber Security, Privacy, and Trust
Programme Proposer:	Myrto Arapinis

STAGE 1: CONSULTATION

Please confirm consultation with relevant stakeholders has taken place.

Stakeholder	Yes	NA
School Director of Professional Services	<input checked="" type="checkbox"/>	<input type="checkbox"/>
School Academic Administration Staff	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Information Services (including Academic Support Librarians)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Student Body (SSLC/Student representatives)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Partner School Staff (E.G. Joint Programmes/shared courses etc)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Employers	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Industry and Professional Bodies	<input checked="" type="checkbox"/>	<input type="checkbox"/>
External Consultation	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Please note any other consultation		

Please provide a brief comment on the consultation process

- This is a new programme developed for a highly specific apprenticeship cohort.
-
- The consultation has been the same as for the full time (non graduate apprenticeship) version of the programme. The GA variant needs also to align to the published Skills Development Scotland GA framework for Cyber Security The GA variation of the programme has been presented to and agreed by SDS that it fully meets the cyber security framework that it aligns to.
- The programme content and delivery model have also been consulted on by the supporting employers including Scottish Government, Morgan Stanley and Tesco Bank.

Drawing from the consultation of the full-time programme

- We have consulted with the student body via our weekly reps meeting and there is strong approval for the creation of this degree.
- Partner Schools providing courses on the degree have been consulted and have agreed to the inclusion of their courses in the DPT.
- We have consulted with employers and industry via the Bayes Centre and City Deal. Currently there is a plan to develop a Level 11 Graduate Apprenticeship version of the programme in cooperation with City Deal. Scottish Government has also expressed interest in the development of the degree.
- Because we are the only Centro of Excellence in Cyber Security Research we consult directly with the national coordinating body involving UK government and GCHQ – we have been encouraged to develop this programme by these bodies.
- **We have consulted with Admissions on controlling intakes on all of our popular MSc courses. This includes this programme. We have agreed to the targets mentioned here and a process that will only consider the most highly qualified candidates and may involve closing the programme early if there is very heavy demand.**

Please provide a brief comment on the consultation process with External consultants

- External consultation has comprised several meetings with our contacts in GCHQ and UK government vis the **National Cyber Security Centre (<https://www.ncsc.gov.uk>)**.

STAGE 2: SCHOOL BOARD OF STUDIES REVIEW AND APPROVAL

Confirmation of approval of the proposal at the School Board of Studies should be entered below.

Date of BoS:
Convener Name:
Comment and Approval (BoS Minute):

STAGE 3: HEAD OF SCHOOL REVIEW AND APPROVAL

Head of School: Johanna Moore <i>Please print name</i>
Comment and Approval:
Signature:

STAGE 4: COLLEGE CURRICULUM APPROVAL BOARD REVIEW AND OUTCOME

Date of CCAB:	
Convener Name:	
Stage 1 Outcome (please select as appropriate)	
Permission to proceed to Stage 2	<input type="checkbox"/>
Permission to proceed to Stage 2 with conditions	<input type="checkbox"/>

Proposal rejected with recommendations	<input type="checkbox"/>
Proposal rejected	<input type="checkbox"/>
Comment:	

Document Control

Date approved: Start date:	Amendments:	Date for next review:
Contact name & role:	Department:	Email:
If you require this document in an alternative format please email: deanqa@exseed.ed.ac.uk		