Board of Studies

Course Proposal Template

PROPOSED COURSE TITLE: Quantum Cyber Security

PROPOSER(S): Petros Wallden(pwallden@inf.ed.ac.uk)

DATE:2018-11-26

Form generated on 2018-11-26by Webmark;User 'pwallden@inf.ed.ac.uk' verified..

SUMMARY

This template contains the following sections, which should be prepared roughly in the order in which they appear (to avoid spending too much time on preparation of proposals that are unlikely to be approved):

1. Case for Support
– To be supplied by the proposer and shown to the BoS Academic Secretary prior to preparation of an in-depth course description

1a. Overall contribution to teaching portfolio

1b. Target audience and expected demand

1c. Relation to existing curriculum

1d. Resources

2. Course descriptor
- This is the official course documentation that will be published if the course is approved, ITO and the BoS Academic Secretary can assist in its preparation

3. Course materials
- These should be prepared once the Board meeting at which the proposal will be discussed has been specified

3a. Sample exam question

3b. Sample coursework specification

3c. Sample tutorial/lab sheet question

3d. Any other relevant materials

4. Course management

- This information can be compiled in parallel to the elicitation of comments for section 5.

4a. Course information and publicity

4b. Feedback

4c. Management of teaching delivery

5. Comments

- To be collected by the proposer in good time before the actual BoS meeting and included as received

5a. Year Organiser Comments

5b. Degree Programme Co-Ordinators

5c. BoS Academic Secretary

[Guidance in square brackets below each item. Please also refer to the guidance for new course proposals at http://www.inf.ed.ac.uk/student-services/committees/board-of-studies/course-proposal-guidelines. Examples of previous course proposal submissions are available on the past meetings page http://web.inf.ed.ac.uk/infweb/admin/committees/bos/meetings-directory.]

SECTION 1 – CASE FOR SUPPORT

[This section should summarise why the new course is needed, how it fits with the existing course portfolio, the curricula of our Degree Programmes, and delivery of teaching for the different years it would affect.]

1a. Overall contribution to teaching portfolio

[Explain what motivates the course proposal, e.g. an emergent or maturing research area, a previous course having become outdated or inappropriate in other ways, novel research activity or newly acquired expertise in the School, offerings of our competitors.]

There is a global intense initiative on Quantum Technologies by governments, big companies

and numerous start-ups. This will change the landscape of research, specifically in Cyber Security, as

Quantum Computation and Quantum Communications are disruptive innovations. UK was the first to realise

the potential new opportunities as well as the threats that come with Quantum Technologies and launched a

270 million EPSRC Quantum Technologies Initiative in 2014. The relevance to the Cyber Security research

was recognised by the Blackett Review (review by the UK government on Quantum Technologies) and

GCHQ. Future research and applications in Cyber Security both in Universities and Industry, would need to

be ready to address, learn and adjust to the quickly developing new Quantum Technologies. By having a

solid background offered by this course, our graduates will be placed in an advantageous position. Moreover,

such a course is likely to attract ambitious students and distinguish our MSc Programme in Security and

Privacy from competitors.

1b. Target audience and expected demand

[Describe the type of student the course would appeal to in terms of background, level of ability, and interests, and the expected class size for the course based on anticipated demand. A good justification would include some evidence, e.g. by referring to projects in an area, class sizes in similar courses, employer demand for the skills taught in the course, etc.]

The main audience will be from students in the new MSc in Security and Privacy. There will be more students (mainly final year undergraduate) with interest in either Computer Security or Quantum Informatics. Students with some background in one of those two fields are likely to attend. (note Computer Security is now 3rd year compulsory course, while the Introduction to Quantum Computing had 45 students).

It is hard to estimate the number of students in the first year it runs. My guess would be O(40) students.

1c. Relation to existing curriculum

[This section should describe how the proposed course relates to existing courses, programmes, years of study, and specialisms. Every new course should make an important contribution to the delivery of our Degree Programmes, which are described at http://www.drps.ed.ac.uk/17-18/dpt/drps_inf.htm.

Please name the Programmes the course will contribute to, and justify its contribution in relation to courses already available within those programmes. For courses available to MSc students, describe which specialism(s) the course should be listed under (see http://web.inf.ed.ac.uk/infweb/student-services/ito/students/taught-msc-2017/programme-guide/specialist-areas), and what its significance for the specialism would be. Comment on the fit of the proposed course with the structure of academic years for which it should be offered. This is described in the Year Guides linked from http://web.inf.ed.ac.uk/infweb/student-services/ito/students.]

This course will be part of the MSc in Security and Privacy.

1d. Resources

[While course approvals do not anticipate the School's decision that a course will actually be taught in any given year, it is important to describe what resources would be required if it were run. Please describe how much lecturing, tutoring, exam preparation and marking effort will be required in steady state, and any additional resources that will be required to set the course up for the first time. Please make sure that you provide estimates relative to class size if there are natural limits to its scalability (e.g. due to equipment or space requirements). Describe the profile of the course team, including lecturer, tutors, markers, and their required background. Where possible, identify a set of specific lecturers who have confirmed that they would either like to teach this course apart from the proposer, or who could teach the course in principle. It is useful to include ideas and suggestions for potential teaching duty re-allocation (e.g. through course sharing, discontinuation of an existing course, voluntary teaching over and above normal teaching duties) to be taken into account when resourcing decisions are made.]

Lectures:20
Tutoring:8

Demonstrating:
Exam Preparation:
Exam Marking:
Other Requirements:

SECTION 2 – COURSE DESCRIPTOR

[This is the official course descriptor that will be published by the University and serves as the authoritative source of information about the course for student via DRPS and PATH. Current course descriptions in the EUCLID Course Catalogue are available at www.euclid.ed.ac.uk under 'DPTs and Courses', searching for courses beginning 'INFR'*]*

2a. Course Title*[Name of the course.]*:

Quantum Cyber Security

2b. SCQF Credit Points:

[The Scottish Credit and Qualifications Framework specifies where each training component provided by educational institutions fits into the national education system. Credit points per course are normally 10 or 20, and a student normally enrols for 60 credits per semester. For those familiar with the ECTS system, one ECTS credit is equivalent to 2 SCQF credits. See also http://www.scqf.org.uk/The%20Framework/Credit%20Points.]

10

SCQF Credit Level:

[These levels correspond to different levels of skills and outcomes, see http://www.sqa.org.uk/files_ccc/SCQF-LevelDescriptors.pdfAt University level, Year 1/2 courses are normally level 8, Year 3 can be level 9 or 10, Year 4 10 or 11, and Year 5/MSc have to be level 11. MSc programmes may permit a small number (up to 30 credits overall) of level 9 or 10 courses.]

11

Normal Year Taken: 1/2/3/4/5/MSc

[While a course may be available for more than one year, this should specify when it is normally taken by a student. "5" here indicates the fifth year of undergraduate Masters programmes such as MInf.]

MSc (Postgraduate)

Also available in years: 1/2/3/4/5/MSc

Different options are possible depending on the choice of SCQF Credit Level above: for level 9, you should specify if the course is for 3rd year undergraduates only, or also open to MSc students (default); for level 10, you should specify if the course is available to 3rd year and 4th year undergraduates (default), 4th year undergraduates only, and whether it should be open to MSc students; for level 11, a course can be available to 4th and 5th year undergraduates and MSc students (default), to 5th year undergraduates and MSc students, or to MSc students only]

UG5

Undergraduate or Postgraduate?

[If the course is only available to MSc students, then it must be classified as a Postgraduate course. All other courses, regardless of level, will be classified as Undergraduate]

Undergraduate

2c. Subject Area and Specialism Classification:

[Any combination of Computer Science, Artificial Intelligence, Software Engineering and/or Cognitive Science as appropriate. For courses available to MSc students, please also specify the relevant MSc specialist area (to be found in the online MSc Year Guide at http://web.inf.ed.ac.uk/infweb/student-services/ito/students/taught-msc-2017/programme-guide/specialist-areas), distinguishing between whether the course should be considered as "core" or "optional" for the respective specialist area.]

Appropriate/Important for the Following Degree Programmes:

[Please check against programmes from http://www.drps.ed.ac.uk/17-18/dpt/drps_inf.htm to determine any specific programmes for which the course would be relevant (in many cases, information about the Subject Area classification above will be sufficient and specific programmes do not have to be specified). Some courses may be specifically designed for non-Informatics students or with students with a specific profile as a potential audience, please describe this here if appropriate.]

Timetabling Information:

[Provide details on the semester the course should be offered in, specifying any timetabling constraints to be considered (e.g. overlap of popular combinations, other specialism courses, external courses etc).]

Should not coincide with any compulsory or suggested course of the MSc Security and Privacy

2d. Summary Course Description:

[Provide a brief official description of the course, around 100 words. This should be worded in a student-friendly way, it is the part of the descriptor a student is most likely to read.]

In this course we cover a broad range of effects that the development of quantum technologies bring on the security and privacy of communication and computation. In particular we consider (i) post-quantum security: security of classical protocols when the adversaries have access to quantum computers or other quantum technologies and (ii) quantumly-enhanced security: when quantum technologies are used by honest parties to achieve better (in terms of security or efficiency) performance. We give an overview of the field, while in each case we focus on selected examples to illustrate how to handle security in a world with quantum technologies.

Course Description:

[Provide an academic description, an outline of the content covered by the course and a description of the learning experience students can expect to get. See guidance notes at: http://www.studentsystems.is.ed.ac.uk/staff/Support/User_Guides/CCAM/CCAM_Information_Captured.html

This course deals with the various effects that developing quantum technologies will have on cyber security. Quantum computing and quantum information theory offers new possibilities (in terms of efficiency and security). Here we examine both the extra attacks that adversaries equipped with quantum technologies can perform and the extra possibilities opened when honest parties use quantum technologies.

The students first will be introduced to quantum information concepts (qubits, mixed states, operations, distance measures) as well as quantum algorithms (factoring, discrete logarithms, search) and their limitations. This will lead to LO1, namely learn the mathematical machinery and the power (and limitations) of quantum information and computation, in view of using these for cyber security.

The second part consists of learning and understanding quantum cryptography and specifically "quantum-key-distribution" protocols, including their security proofs and the how different implementations affect the performance (see LO4). The limitations (practical and theoretical) of quantum cryptography will also be analysed here (including impossibility results).

The third part deals with generalising classical notions such as encryption, authentication and secure delegated computation to quantum information. Introducing students in these concepts prepares them for the next generation of quantum cyber security that is bound to become relevant when large(r) quantum computers are constructed (LO5).

Finally, the last part of the course focuses on classical protocols and their security under quantum attacks. A cryptosystem based on the learning-with-errors problems will be introduced as a (key) example of this possibility (LO2). Furthermore, general quantum attacks (superposition attacks, the quantum random oracle model, etc) will be introduced and students will learn to analyse general quantum attacks on a given classical protocol (LO3).

Pre-Requisite Courses:

[Specify any courses that a student must have taken to be permitted to take this course. Pre-requisites listed in this section can only be waived by special permission from the School's

Curriculum Approval Officer, so they should be treated as "must-have". By default, you may assume that any student who will register for the course has taken those courses compulsory for the degree for which the course is listed in previous years.

Please include the FULL course name andcourse code].

Co-Requisite Courses:

[Specify any courses that should be taken in parallel with the existing course. Note that this leads to a timetabling constraint that should be mentioned elsewhere in the proposal.Please include the FULL course name and course code].

Either having done a Computer Security course (as INFR10067) or taking the Research Methods in Security, Privacy & Trust (compulsory MSc Security and Privacy course) or having done a Quantum Computing course (INFR11067 or equivalent)

Prohibited Combinations:

[Specify any courses that should not be taken in combination with the proposed course.Please include the FULL course name and course code].

Other Requirements:

[Please list any further background students should have, including, for example, mathematical skills, programming ability, experimentation/lab experience, etc. It is important to consider that unless there are formal prerequisites for participation in a course, other Schools can register their students onto our courses, so it is important to be clear in this section. Also be aware that MSc students are unlikely to have the pre-requisite courses, so alternative knowledge should be recommended. If you want to only permit this by special permission, a statement like "Successful completion of Year X of an Informatics Single or Combined Honours Degree, or equivalent by permission of the School." can be included.]

Either having done a Computer Security course (as INFR10067) or taking the Research Methods in Security, Privacy & Trust (compulsory MSc Security and Privacy course) or having done a Quantum Computing course (INFR11067 or equivalent)

Available to Visiting Students: Yes/No

[Provide a justification if the answer is No.]

The level of the course is tuned for Postgraduate, and visiting students are mainly undergraduate

2e. Summary of Intended Learning Outcomes (MAXIMUM OF 5):

[List the learning outcomes of the course, emphasising what the impact of the course will be on an individual who successfully completes it, rather than the activity that will lead to this outcome. Further guidance is available from https://canvas.instructure.com/courses/801386/files/24062695]

On completion of this course, the student will be able to

* Understanding the power and limitations of quantum computation and obtain knowledge and ability to use the basic mathematical formalism for quantum information and quantum cryptography
* Understanding of what it takes for a classical cryptosystem to be secure against quantum attacks
* Develop the ability to analyse quantum attacks to classical protocols
* Be able to understand the security of quantum cryptography and to analyse how different implementations affect the performance
* Understand security notions for quantum information, such as encryption and authentication, and their application to blind quantum computation

Assessment Information

[Provide a description of all types of assessment that will be used in the course (e.g. written exam, oral presentation, essay, programming practical, etc) and how each of them will assess the intended learning outcomes listed above. Where coursework involves group work, it is important to remember that every student has to be assessed individually for their contribution to any jointly produced piece of work. Please include any minimum requirements for assessment components e.g. student must pass all individual pieces of assessment as well as course overall].

Written Exam: 90%

A written exam that covers all four parts of the course and that tests all the LOs. The exam contains a small theory part, testing the knowledge of key topics of the course and the remaining exam requires understanding and being able to apply the knowledge on concrete examples.

Other (coursework): 10%

A single coursework, that checks the understanding of students in LO 1-5, and goes beyond the material presented in the lectures by asking questions that require deeper thought or research.

Assessment Weightings:

Written Examination: 90%

Practical Examination: 0%

Coursework: 10%

Time spend on assignments:

[Weightings up to a 70/30 split between exam and coursework are considered standard, any higher coursework percentage requires a specific justification. The general expectation is that a 10-point course will have an 80/20 split and include the equivalent of one 20-hour coursework assignment (although this can be split into several smaller pieces of coursework. The Practical Examination category should be used for courses with programming exams. You should not expect that during term time a student will have more than 2-4 hours to spend on a single assignment for a course per week. Please note that it is possible, and in many cases desirable, to include formative assignments which are not formally assessed but submitted for feedback, often in combination with peer assessment.]

90/10

Academic description:

[A more technical summary of the course aims and contents. May include terminology and technical content that might be more relevant to colleagues and administrators than to students.]

This course deals with the various effects that developing quantum technologies will have on cyber security. Quantum computing and quantum information theory offers new possibilities (in terms of efficiency and security). Here we examine both the extra attacks that adversaries equipped with quantum technologies can perform and the extra possibilities opened when honest parties use quantum technologies. The students first will be introduced to quantum information concepts (qubits, mixed states, operations, distance measures) as well as quantum algorithms (factoring, discrete logarithms, search) and their limitations. This will lead to LO1, namely learn the mathematical machinery and the power (and limitations) of quantum information and computation, in view of using these for cyber security. The second part consists of learning and understanding quantum cryptography and specifically “quantum-key-distribution” protocols, including their security proofs and the how different implementations affect the performance (see LO4). The limitations (practical and theoretical) of quantum cryptography will also be analysed here (including impossibility results). The third part deals with generalising classical notions such as encryption, authentication and secure delegated computation to quantum information. Introducing students in these concepts prepares

them for the next generation of quantum cyber security that is bound to become relevant when large(r) quantum computers are constructed (LO5).

Finally, the last part of the course focuses on classical protocols and their security under quantum attacks. A cryptosystem based on the learning-with-errors problems will be introduced as a (key) example of this possibility (LO2). Furthermore, general quantum attacks (superposition attacks, the quantum random oracle model, etc) will be introduced and students will learn to analyse general quantum attacks on a given classical protocol (LO3).

Syllabus:

[Provide a more detailed description of the contents of the course, e.g. a list of bullet points roughly corresponding to the topics covered in each individual lecture/tutorial/coursework. The description should not exceed 500 wordsbut should be detailed enough to allow a student to have a good idea of what material will be covered in the course. Please keep in mind that this needs to be flexible enough to allow for minor changes from year to year without requiring new course approval each time.]

- Quantum Information: qubits, mixed states, operations, distance measures, teleportation, no-cloning, entropy

- Quantum Algorithms: Analysis of which problems and in what extend quantum computers offer speed-up compared to classical computers (but not detailed description of each quantum algorithms)

- Quantum Enhanced Security I: The BB84 quantum key distribution protocol. Security proof and the effects of different implementations

- Quantum Enhanced Security II: The impossibility of, information theoretic secure, quantum bit-commitment (and related impossibilities)

- Quantum Enhanced Security III: Quantum encryption and quantum authentication. Definitions and protocols.

- Quantum Enhanced Security IV: (Advanced topic) Blind quantum computing

- Post-quantum Cryptography: The Learning-with-Errors cryptosystem (introduction of the problem and its use as a cryptosystem, analysis why such cryptosystem is believed to be secure against quantum attackers)

- Quantum Cryptanalysis: Superposition attacks, quantum indistinguishability and the quantum random oracle model.

Relevant QAA Computing Curriculum Sections:

[Please see http://www.qaa.ac.uk/en/Publications/Documents/SBS-Computing-consultation-15.pdf to check which section the course fits into.]

Graduate Attributes, Personal and Professionalskills:

[This field should be used to describe the contribution made to the development of a student's personal and professional attributes and skills as a result of studying this course – i.e. the generic and transferable skills beyond the subject of study itself. Reference in particular should be made to SCQF learning characteristics at the correct level http://www.sqa.org.uk/files_ccc/SCQF-LevelDescriptors.pdf].

Reading List:

*[Provide a list of relevant readings. See also remarks under **3d**.]*

The lecture notes as main source and as supplementary reading:

Quantum Computation and Quantum Information by Nielsen and Chuang

Quantum Information by Stephen Barnett

Post-Quantum Cryptography Editors Daniel J. Bernstein, Johannes Buchmann and Erik Dahmen

Breakdown of Learning and Teaching Activities:

[Total number oflecture hours and tutorial hours, with hours for coursework assignments.]

[The breakdown of learning and teaching activities should only include contact hours with the students; everything else should be accounted for in the Directed Learning and Independent Learning hours.

The total being 10 x course credits. Assume 10 weeks of lectures slots and 10 weeks of tutorials, though not all of these need to be filled with actual contact hours. As a guideline, if a 10-pt course has 20 lecture slots in principle, around 15 of these should be filled with examinable material; the rest should be used for guest lectures, revision sessions, introductions to assignments, etc. Additional categories of learning and teaching activities are available, a full list can be found at:

http://www.euclid.ed.ac.uk/Staff/Support/User_Guides/CCAM/Teaching_Learning.htm]

Lecture Hours: 20hours

Seminar/Tutorial Hours: 8 hours

Supervise practical/Workshop/Studio hours: hours

Summative assessment hours: hours

Feedback/Feedforward hours: hours

Directed Learning and Independent Learning hours: hours

Total hours: 29.00 hours

You may also find the guidance on 'Total Contact Teaching Hours' and 'Examination & Assessment Information' at:http://www.studentsystems.ed.ac.uk/Staff/Support/User_Guides/CCAM/CCAM_Information_Captured.html

Keywords:

[A list of searchable keywords.]

cyber security, quantum cryptography, quantum computation

SECTION 3 - COURSE MATERIALS

3a. Sample exam question(s)

[Sample exam questions with model answers to the individual questions are required for new courses. A justification of the exam format should be provided where the suggested format non-standard. The online list of past exam papers gives an idea of what exam formats are most commonly used and which alternative formats have been http://www.inf.ed.ac.uk/teaching/exam_papers/.]

Here is one exam question that has two sub-parts (the first is theory from the background on quantum information section of the course and the second is not a theory question and is on the post-quantum security section).

(i) Consider the quantum one-time-pad. Write the quantum state that a forger intercepting a quantum ciphertext has (without knowing the keys k_1,k_2), and prove that the quantum one-time-pad is secure. Recall that the ciphertext is of the form X^{k_1}Z^{k_2} |\psi>.

(ii) Consider a hash function h with range in {0,1}^16.

(a) Model the function as a random function (random oracle), and estimate how many calls to the oracle a classical PPT adversary needs to obtain a bit string starting with four zeros (i.e. h(x)=0000b_5b_6 ... b_16), with probability of success greater than 1/2.

(b) Now consider a quantum adversary QPT, with access to a quantum version of this function modelled as a quantum random oracle. Using Grover's search algorithm find how many calls to the quantum oracle are required to obtain a bit string starting with four zeros (i.e. h(x)=0000b_5b_6 ... b_16), with probability of success close or greater than 1/2.

Answers (brief):

(i) One needs to describe the forger's state as an ensemble of states (mixed state) that with probability 1/4 is any of the four states |psi>,X|psi>,Z|psi>,XZ|psi> depending on the values of the keys k_1,k_2. By computing the resulting mixed state for a general (unknown) state |psi>=a|0>+b|1> we can see that averaging over the unknown keys k_1,k_2 leads to the totally mixed state for any unknown plaintext quantum state |psi>. It is therefore independent of the plaintext and thus secure.

(1/3 of marks of the question goes here)

(ii) (a) The probability of obtaining a string that starts with 0000 with one call to the oracle is 1/2^4=1/16. It is easy to see that one requires 8 calls to the oracle to have probability 1/2 to have at least one bit-string starting with 0000.

(ii)(b) One needs to model the question as a search algorithm where the solution is one of 16 places (4-qubits Grover search). Then the algorithm starts with preparing the equal superposition, querying the oracle in this sate, and using the quantum random oracle as the oracle of Grover's search. By applying Grover's algorithm with two iterations (and measuring after these two iterations) one obtains a bit-string starting with 0000 with probability of success 0.47. With three iterations instead, this probability becomes 0.9.

3b. Sample coursework specification

[Provide a description of a possible assignment with an estimate of effort against each sub-task and a description of marking criteria.]

The assignment will have two parts.

Part I: An essay on one key subject, asking the students to go beyond the lectures material using as basis some references provided.

Example: In the lectures we have seen that information theoretic secure (ITS) bit commitment is impossible, even if we use quantum resources. There was a strong impossibility result ruling out all such protocols. However, if one is prepared to relax some conditions of the theorem, one can achieve such task. One can do this e.g. by imposing relativistic constraints, or by assuming adversaries with bounded quantum memory, etc (see refs). Choose one of these approaches, and give a short review of a bit commitment protocol (from literature) explaining clearly how the impossibility result is evaded.

50% of assignment

Part II: Two-three questions/exercises requiring a bit more creativity than standard tutorial questions. (50% of assignment)

Example (one such question): Consider a QKD protocol where Alice sends one of two possible states {|0>,|+>} to Bob. Alice in order to send the bit 0 prepares the state |0> and to send the bit 1 sends the state |+>. Bob randomly measures in the X or Z basis. In an honest run, if he gets either the state |1> or the state |->, he knows that Alice sent a state from the other basis (since it is impossible that Alice sent the state |0> and Bob obtained for measurement outcome the state |1>, etc). Bob announces the positions for which he is certain on Alice's sent state and they keep only those (raw key).

(i) In an honest run, which is the expected fraction of positions that Bob got a definite outcome? (1/2 marks of question)

(ii) We assume for now that Bob indeed had that number of definite outcomes. By checking a random small fraction (parameter estimation) they evaluate the QBER (quantum-bit error-rate). Is such protocol secure if the QBER is zero, and why? (1/4 marks of question)

(iii) Assuming that the fraction of bit positions with definite outcomes are much fewer, but still with QBER being zero. Give an attack that Eve can do and cheat with certainty and estimate the fraction of positions that Bob detects definite outcomes in this case. (1/4 marks of the question)

3c. Sample tutorial/lab sheet questions

[Provide a list of tutorial questions and answers and/or samples of lab sheets.]

3d. Any other relevant materials

[Include anything else that is relevant, possibly in the form of links. If you do not want to specify a set of concrete readings for the official course descriptor, please list examples here.]

SECTION 4 - COURSE MANAGEMENT

4a. Course information and publicity

[Describe what information will be provided at the start of the academic year in which format, how and where the course will be advertised, what materials will be made available online and when they will be finalised. Please note that University and School policies require that all course information is available at the start of the academic year including all teaching materials and lecture slides.]

4b. Feedback

[Provide details on feedback arrangements for the course. This includes when and how course feedback is solicited from the class and responded to, what feedback will be provided on assessment (coursework and exams) within what timeframe, and what opportunities students will be given to respond to feedback.

The University is committed to a baseline of principles regarding feedback that we have to implement at every level, these are described at http://www.docs.sasg.ed.ac.uk/AcademicServices/Policies/Feedback_Standards_Guiding_Principles.pdf.

Further guidance is available from http://www.enhancingfeedback.ed.ac.uk/staff.html.]

4c. Management of teaching delivery

[Provide details on responsibilities of each course staff member, how the lecturer will recruit, train, and supervise other course staff, what forms of communication with the class will be used, how required equipment will be procured and maintained. Include information about what support will be required for this from other parties, e.g. colleagues or the Informatics Teaching Organisation.]

SECTION 5 - COMMENTS

[This section summarises comments received from relevant individuals prior to proposing the course. If you have not discussed this proposal with others please note this].

5a. Year Organiser Comments

[Year Organisers are responsible for maintaining the official Year Guides for every year of study, which, among other things, provide guidance on available course choices and specialist areas. The Year Organisers of all years for which the course will be offered should be consulted on the appropriateness and relevance on the course. Issues to consider here include balance of course offerings across semesters, subject areas, and credit levels, timetabling implications, fit into the administrative structures used in delivering that year.]

5b. BoS Academic Secretary

[Any proposal has to be checked by the Secretary of the Board of Studies prior to discussion at the actual Board meeting. This is a placeholder for their comments, mainly on the formal quality of the content provided above.]
