Code of Practice for the Oversight and Use of Security-Sensitive and Other Sensitive Research Material.

1. Background.

In 2008 a PhD student and a colleague at Nottingham University were arrested and detained for 7 days for suspected involvement in Islamic terrorism. Their supposed 'crime' – which was reported to police by a University manager – was to download a document which, it later transpired, was freely available for sale from a well-known internet bookseller. This has become known as the "Nottingham Case". Subsequent cases have involved, amongst others, staff at the Universities of Oxford and Liverpool.

The case raised the profile of dilemmas that can face legitimate researchers working on security- and other sensitive topics, and highlighted the need for some guidance for researchers and Universities. In October 2012 Universities UK published *Oversight of security-sensitive research material in UK universities: guidance*, following discussions among stakeholders in security research that had been active in the UK since 2008. That document has been used to inform the content of this Code of Practice.

The need for a Code of Practice on this subject has been further reinforced by the UK government's Prevent Strategy under its anti-terrorism legislation (Counter Terrorism and Security Act 2015) which requires HEIs to 'have due regard to the need to prevent people being drawn into terrorism'. Whilst research involving other sensitive areas is not part of the Prevent Duty, it can lead to similar problems for researchers. We have therefore followed UUK guidance and included it in this Code of Practice. The views of CCCU researchers, gathered at the RKE Forum on this topic held in October 2015, have also informed the content of this document.

The overarching principle within this Code of Practice is that all research carried out by staff or students at this University must take place within the boundaries of United *Kingdom law as it stands at the time the research is being carried out.*

2. The Issues.

- Universities play a vital role in carrying out research on issues where security-sensitive material is relevant. Careless circulation of this material can lead to misinterpretation by the authorities, putting researchers at risk of arrest and prosecution.
- Potential problems for researchers in justifying the legitimacy of materials held on personally-owned computers highlights the need for guidance on the storage and circulation of security-sensitive material.
- This indicates a clear need for a system of safeguards to protect legitimate research from official intrusion and misinterpretation, and to respond rapidly and effectively when problems occur.
- The system of safeguards will have resource implications (IT hardware and support, training etc).
- Defining what falls into the categories of 'security-sensitive' and 'other legally sensitive' research. These might include (amongst others):

  Security-sensitive

  - Terrorism
  - Other extremist groups
  - Defence-commissioned research
  - Computer encryption/decryption

  Other legally sensitive

- Child abuse
- Vulnerable adult abuse
- People trafficking
- Money laundering
- Exploitation (including cyber-)

These 'other legally sensitive' research areas are, in the main, those that may involve accessing on-line and other resources that are subject to monitoring by various law enforcement agencies.

- The above lists emphasise the need to avoid stigmatising particular groups.

- The need for complementary safeguards for non-researchers – professional services staff, undergraduate students – who may use University computers to access security sensitive material either as part of their jobs or out of curiosity.

3. How these issues will be handled at CCCU.

3.1 *Identifying sensitive research*.

The University now requires all academic staff and research students to declare that they are using security or other sensitive information in their research. This is in keeping with openness in research, and is intended to protect researchers by preventing (or at least reducing) the misidentification of their information-gathering as suspect or criminal. To overcome the possibility of stigmatizing specific groups (a point raised at the RKE Forum), we have noted the UUK guidance in using our ethical review procedures to identify research that falls into this category.

This has necessitated the introduction of a separate but related extension to our ethical review policy which previously only required ethical review for research or knowledge exchange studies involving human participants or sentient animals. The revised system requires all researchers to declare any proposed use of security or other sensitive material at an early stage as an extension of the existing ethical review process.

3.2 Pre-study notification of sensitive research.

Staff or research students contemplating research falling into the sensitive categories will often legitimately access sensitive material during the process of compiling their research proposals. In so doing they will face the same issues as those actually engaged in a research study. This highlights the need to notify the University so that, for their own protection against unwarranted suspicion, their access to these materials can be registered as *bona fide*.

Before starting to access the sensitive materials via the University IT facilities, researchers (staff or research students) **are required to complete** a Sensitive Research Checklist [Appendix 1 ***to follow in due course once this Code of Practice approved***]. At this point it may be advisable to secure appropriate legal advice before forwarding this Checklist to Research & Enterprise Development via their line manager or academic supervisor. The Checklist will be reviewed by a sub-group (at least three members) of the Research Ethics and Governance Committee chaired by the PVC (Research & Enterprise). After review they will be entered as development studies into the register of sensitive research maintained by the Research Governance Manager.

3.3 *Reviewing and registering sensitive research.*

Once a research proposal has been developed and agreed by an academic supervisor (for students) or Head of School (staff) a Proportionate Ethical Review Checklist must be completed for EVERY research or knowledge transfer project (WHETHER OR NOT it involves human or animal participants), to identify any proposed use of, or access to, security or other sensitive material. As the UUK guidance points out, "*the ethical justification for doing this is straightforward: unauthorised acquisition and use of security-sensitive information can carry risks to the public, and even legitimate researchers can be suspected of obtaining it and using*

it in ways that can be harmful, with costs to those researchers. Oversight helps to prevent both kinds of harm".

The Proportionate Ethical Review Checklist has been revised for this purpose, and is attached at Appendix 2 [*to follow in due course once this Code of Practice approved*]. **NB: The revised Checklist will take account of any review previously undertaken at the pre-study stage as at 3.2 above.**

Completed Proportionate Ethical Review Checklists will continue to be sent to Research & Enterprise Development (RED) in the first instance. These will be processed as follows:

- Studies that involve human participants only will continue to undergo proportionate ethical review.
- Studies that involve human participants and security or legally sensitive materials will be required to undergo a full review by the relevant Faculty Research Ethics Committee. They will also be registered as full security or other sensitive research studies by the Research &b Enterprise development.

The registration of all studies involving security or legally sensitive research categories at the ethical review stage is mandatory. Failure to comply will be treated as research misconduct and subject to disciplinary action. Once a study becomes registered as security or other sensitive research, RED will notify the line manager or academic supervisor of the lead researcher concerned.

All researchers whose studies are registered as security or other sensitive research will be offered access to a centrally managed 'safe-storage' facility on a voluntary basis.

3.4 ***Provision of a 'safe-storage area' on a central computing server.***

Researchers who take up the offer of access to 'safe storage' will be issued with a link to a password-protected documents file on a secure centrally-managed server to which they can upload their sensitive research documents. These documents can be accessed only by the research team, and are subject to a norm of non-circulation. **The use of the 'safe store' facility is voluntary, but is strongly recommended for all researchers using security and other sensitive materials**.

Material kept on the secure server will not necessarily be classified as secret; rather it will be material that, if found on personal computers or as attachments in covertly observed email traffic, may throw suspicion on the computer owners or senders of emails. The purpose of the 'safe store' is to identify the material as being legitimately stored for research and to keep it out of any further circulation. In addition to documents that were originally in electronic form, the store will help to discourage the separate storage of hard copy by storing scanned versions of paper documents that might look suspicious to an outsider if found on a researcher's desk. Whilst not typically functioning as a repository for an individual researcher's writing about security-sensitive material, the 'safe store' could take on this role if the researcher considers that to be appropriate. Data stored in the secure area will be subject to locally agreed data storage and retention regulations. [*Note to Committee: Guidelines for accessing and using the safe area to be developed in conjunction with Computing Services*]

The Designated Staff overseeing the store will only know the titles of documents on the server and the names of researchers. In this way research is kept secure and at arm's length from police, in return for openness on the part of researchers about their use of security and other sensitive material, all of which they keep in the store. Material deposited in the store is deemed to have a legitimate research purpose unless Designated Staff cannot confirm its status as registered material under 3.2 and 3.3 above, or identify the relevant researcher responsible.

3.5 ***Identification and roles of 'Designated staff'.***

The UUK guidance recommends the identification of designated staff whose roles are to manage the 'safe store' and to be the first point of contact for both internal (University) and external (police etc) enquiries about suspect security and other sensitive material associated with the University or a member of its staff or a research student. The CCCU Designated Staff are:

Pro Vice-Chancellor (Research & Enterprise) responsible for:

- overall management of the oversight of security and other sensitive research
- senior-level liaison with police and security service enquiries

University Solicitor responsible for:

- initial point of contact for external enquiries (as above)

Research Governance Manager responsible for:

- identification of sensitive research through the extended ethical review process
- registering security and other sensitive research studies
- day-to-day management of the content of the central 'safe store'
- initial point of contact for internal enquiries (as above)

3.6 ***Handling internal and external enquiries.***
Enquiries will be handled as recommended in the UUK guidance.

3.6.1 Internal enquiries. Internal enquiries will most likely be triggered by the unexpected discovery of security or other sensitive material in an inappropriate place. Whilst the requirements for using the 'safe store' make the unexpected discovery of such material in an inappropriate electronic location less likely, hard copy material might still be in circulation and raise questions even though storage in this format is discouraged (see 3.3 above).

Anyone making a discovery of possibly suspicious material should first take the material to campus security, who will have been briefed about the policy on security-sensitive material. They will then contact their own line manager and the Research Governance Manager (RGM) for verification (or otherwise) that the researcher concerned is undertaking a registered study allowing legitimate access to the material in question. The RGM will check the register of declared studies, and consult the researcher and then the researcher's line manager or academic supervisor as appropriate with a view to early clarification of the situation. The PVC (Research & Enterprise) will also be informed at this stage. These steps must be undertaken before the police are contacted.

3.6.2 External enquiries. These are most likely to come direct from the police following their own discovery, or an externally reported discovery, of security or other sensitive material associated with the University or one of our researchers. The University Solicitor's Office (USO) should be their first point of contact. The USO will contact the RGM, who will check the register of declared studies, and consult the researcher and then the researcher's line manager or academic supervisor with a view to early clarification of the situation. The PVC (Research & Enterprise) will also be informed at this stage.

The local police have been made aware of our procedures in this regard as part of our routine engagement with the police on campus safety, crime prevention and our Prevent Duty. This includes contact details – phone and email - for the USO. It is hoped that by being properly briefed in this way, the police are more likely to treat suspect university-associated material as innocent until proven otherwise.

3.7 ***Subsequent actions.***

3.7.1 Internal enquiries. Where the research material in question is proved to be legitimately

held, no further action will be necessary. Where the research material in question is found to be unregistered not otherwise legitimately held, disciplinary action for research misconduct may be taken.

3.7.2 External enquiries. Failure to justify the legitimacy of the research material in question may result in legal action being taken by the police. The University may also take disciplinary action for research misconduct.

4. Complementary safeguards.

There is a need for complementary safeguards to protect from external scrutiny and arrest any non-researchers – professional services staff, undergraduate students – who may access security sensitive material either as part of their jobs or out of curiosity. These individuals would not normally be subjected to a research ethics process or checks by designated staff to clear the material of suspicion. The University's Regulations on the Acceptable Use of University Information Technology, which covers usage by both staff and students, will need to be/have therefore been revised. Failure to comply with the Regulations can result in withdrawal of IT access and the possibility of disciplinary action if deemed appropriate.

This approach has been taken in line with the UUK guidance which recommends that:

"The right response to the danger of official misinterpretation of this material is not to create more central stores for non- researchers. Rather, pointed guidelines are needed for all internet users at universities and more exacting conditions for acquiring email accounts at, and internet access from, universities. University guidance for all internet users can call attention to the risks of visiting and downloading from jihadist websites. Behaviour that seems to ignore this advice might be punished with the loss of email privileges."

In summary, the message to non-researchers as defined above is that for their own protection they should avoid accessing online material which may invite the attention of the law enforcement agencies.

5. Resources and training.

This Code of Practice recognises that there are resource implications for the University. These fall into two identified areas, IT hardware/software and staff costs, and training. Detailed information on the costs of these will be the subject of a separate paper submitted to the Senior Management Team.

The UUK guidance suggests that a training programme should include:

- *a review of current terrorism legislation relevant to research*
- *suggested contents for forms (electronic and paper) for an ethics approval process*
- *suggested internet user advice*
- *what secure server contents would look like when accessed by an ethics officer*
- *what secure server contents would look like when accessed by a researcher*
- *what designated staff should do in the case of a query about security-sensitive research material from within their university*
- *what designated staff should do in the case of a query from outside their university*

The training would probably also involve information for IT officers about the hardware and software necessary for a secure, central storage system.

Training within the University will be via the Researcher Development Programme, and via the Staff Development Programme.

6. Appendices.

Appendix 1 Sensitive Research Checklist (to follow)

Appendix 2 Amended Proportionate Ethical Review Checklist (to follow)

Appendix 3 Amended Ethical Review Flowchart (to follow)

Roger Bone
Research Governance Manager
20 December 2016