Storage of potentially sensitive research materials

Name …….. UG / PGT / PGR / (S)RA / Faculty / Other

Short title of project ……..……...……..…….…….…....

Name of Supervisor / PI / Lab leader:……..……..……. School ……

Nature of materials: Health / Personal / Biomedical / Commercial / Government classified / Legal or criminal / Terrorism or political

---

1. Brief description of the sensitive materials:

……..……

……..……

……..……

……..…… ……

2. Have you completed any Confidentiality Declarations or Non-Disclosure Agreements in respect of the materials? **Yes/No**

If so, please attach copies of relevant NDAs and confidentiality declarations to this form.

3. Where will copies of the materials be stored during the project/dissertation/research?

Include all locations, including any personal copies or off-site backups

……..……

……..……

……..……

……..……

4. What will happen to these materials at the end of the project?

……..……

……..……

……..……

5. Do other people have access to any of these locations? **Yes/No**

If so, list names below:

……..……

6. What physical measures are used to protect potentially sensitive (hardcopy) documents?

……..……

……..……

7. Are the digital materials protected by passwords (additional to your UEA login)? **Yes/No**

8. Are the digital materials encrypted? **Yes/No**

If so, please describe the mechanism (e.g. 7z, FileVault, TruCrypt).

……..……

Approval

Approved **Yes No** Signature **…….** Date…….…..……

Return completed form to the Chair, CMP Ethics Committee (via CMP/MTH General Office S2.45)

Revised May 2013

Notes for Guidance

Nature of materials

Please identify which of these general categories the materials fall into.

1. Brief description of the sensitive materials

Please provide a brief overview of the general type and likely quantity of potentially sensitive material. The purpose of this description is to allow the University to respond appropriately to any requests for information or FOI request relating to this material.

Example descriptions might be: “approx. 10,000 child pornography images”; “’terrorist manuals’ and military training documents used by insurgent groups in several conflicts since 1990”; “commercially sensitive material (approx. 500MB, mostly binary files) from Gazprom – note that the identity of the client is confidential”, “diet and lifestyle records from approx. 5,000 NHS patients”, “classified documents from a government agency”.

2. NDAs and Confidentially Declarations

The purpose of this description is to allow the University to respond appropriately to any requests for information or FOI request relating to this material.

3. Where will copies of the materials be stored?

Please list all the places where potentially sensitive materials will be stored. If copies are kept on

4. What will happen to these materials at the end of the project?

Plans for the management and eventual disposal of research materials at the end of a project are often neglected. It is important to specify how long materials will be kept, in what form, their location, and how they will be eventually destroyed.

5. Do other people have access to any of these locations?

These two questions provide a check to ensure that potentially sensitive digital materials will be stored and managed appropriately, and that it is clear who is allowed access to them.

6. What physical measures are used to protect potentially sensitive research materials and hardcopy documents?

This question provides a check to ensure that hardcopy documents or other physical research materials are appropriately protected. For example: “hardcopy documents and original survey results will be stored in a locked filing cabinet in ECB 1.17, which has swipecard access”, “samples will not be removed from BMRC”.

7. Are the digital materials protected by passwords (additional to your UEA login)?

8. Are the digital materials encrypted?

These questions provide a check that materials that are sufficiently sensitive to need protection additional to the normal UEA measures are protected appropriately. If you are uncertain about the level of protection offered by the various technical security measures available. These range through password-protected documents, two-factor authentication, file systems encrypted at the operating system level (Q7), the encryption of key files or directories with third-party tools (Q8).