Data Protection Roadshow – 14 March 2012

Questions and Answers

1. **How do people lose personal data?**

Personal data can be accidentally or, worse, deliberately compromised in a number of ways; some examples are:

- Leaving paper records containing personal data on public transport or in a taxi;
- An unencrypted laptop, mobile phone or USB stick containing personal data stolen from a house or car or lost;
- Marking a student's work on public transport in view of third parties who can clearly read the document;

If personal data that the College holds is accidentally or deliberately compromised, we would be in breach of principle 7 of the Data Protection Act. Appropriate technical and organisational measures must be taken to prevent unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The College has a Data Loss Procedure which should be followed if personal data is accidentally or deliberately compromised. It can be found on Policy Zone at the following link: http://www.kcl.ac.uk/college/policyzone/index.php?id=458

2. **How can you wipe hard drives in a controlled way?**

Hard disks of computers being disposed must also be made incapable of retrieving the data. Software for doing this is Boot and Nuke can be downloaded and run to generate a bootable USB stick. This USB stick should then be placed in the PC of the computer whose hard drive you want to wipe and reboot. Note you will need your BIOS settings adjusted to boot from a USB stick and once the program is running enter "dod". Note a floppy drive can also be created if the PC is very old.

3. **Under Copyright legislation, are we allowed to send links to the College's Regulations to third parties?**

Yes, the College owns the copyright of its Academic and Related Regulations, so we can do what we want with them. The Regulations are published on our website so links to the document can be forwarded to third parties.

4. **How should we dispose of electronic media such as video tapes, cassette tapes and CD's which contain data such as oral exams?**

Please refer to your School or Department IT support first before destroying any data. Where a data media destruction service exists in the College it must be utilised such as for CD's, DVD's, floppy drives, DAT tapes and Video tapes. Facilities available vary from campus to

campus and if media destruction is not available these items can be disposed of as hazardous waste. Contact your Site Services office for details of local arrangements.

If no services exist then the media must be destroyed and disposed of in accordance with your sites policy of disposal of hazardous waste. It is recommended that hard drives of computers incapable of being erased are removed and locked away until they can be destroyed.

5. Should monitoring data such as ethnicity information be available to all staff that have access to SITS, the student record database?

Good question. We have raised this with the relevant department and when we get an answer we will publish it here.

6. What information about students can you provide over the phone to third parties including parents?

Information relating to students should not be disclosed without their consent. Even confirming or denying that a student is studying at the College *could* infringe their privacy rights. If a request is received over the telephone, ask for details in writing. Contact the student to obtain permission before realising the information, or if there are serious concerns about a student's health or well-being, ask for contact details and pass the details to the student.

Simply confirming a students' degree award (2.1, 2.2 etc) is permitted as the College considers this information to be in the public domain already. Any further detail about a students' time at the College should not be disclosed.

If the police or other organisation with crime prevention, tax collecting or law enforcement functions, such as the Department for Work and Pensions or Local Government Benefit Fraud sections, contact the College asking for information about a student, do not provide information over the telephone.

Ask for the request in writing, and ensure that you are confident about the requester's identity. Also, ask for details of the specific legislation under which they are requesting the information and why they need it. Do not disclose any more personal information than has been requested for the stated purposes and record the details of the request and the decision regarding disclosure in case of future enquiries.

7. What does the term redaction mean?

Redaction means to select or adapt (by obscuring or removing) sensitive information from a document prior to publication or release. We use Adobe Professional as it also removes the metadata when we redact.

8. What information is redacted from disclosures in response to requests for information?

In practice very little information is redacted from responses to subject access requests under the Data Protection Act 1998. The majority of information is disclosed; however any third party personal information is removed where we do not have the permission of the individual to disclose it.

9. What information relating to students should be retained on their student file?

Please find guidance at the following links:

Management of a student record: http://www.kcl.ac.uk/library/info-management/guidance/student.pdf

Content of a student record: http://www.kcl.ac.uk/library/info-management/guidance/checklist.pdf

Email management: http://www.kcl.ac.uk/library/info-management/guidance/email.pdf

10. Are emails deleted in Outlook, deleted from the College's systems entirely?

Not necessarily as they may still be available on backup tapes. To date however we have not disclosed anything that has been stored on back up tape. This has been seen as 'disproportionate effort' under the Data protection Act 1998, which means that the College does not have to undertake the search. This follows the ruling in the court case of *Ezsias v The Welsh Ministers.*