Data Protection Roadshow – 18 April 2012

Questions and Answers

1. **Can a third party ask for someone else's personal information under the Subject Access Request process (Data Protection Act 1998)?**

No, the subject access request process is for a 'subject' to request their own personal information. There are circumstances where a subject can give their permission for a third party to request information on their behalf e.g. a solicitors. Written authority from the data subject must be provided along with proof of identity. Third parties can request any information under the provisions of the Freedom of Information Act 2000. Requests might sometimes include third party personal information however Section 40 (Personal information) of the FOIA exempts personal information being disclosed where permission has not been provided.

2. **Who are likely requesters under the Freedom of Information Act 2000?**

The FOIA is applicant and purpose blind so anyone from anywhere can request information from the College. In 2011 42% of requesters were individual members of the public and 25% of requests came from journalists.

3. **I have to change my password every 3 months but my colleague sat next to me never has to change their password?**

If your colleague works for Kings College Hospital, they will have different password procedures.

4. **Mobile devices – if you are checking a work email on your mobile phone does it have to be encrypted?**

If the emails are retained on the mobile phone and contain personal data, then yes it should be encrypted. If the emails are not retained on the mobile phone, then no it does not have to be encrypted but it should be password protected.

5. **Is storing information in the "Cloud" secure? Can you password protect a document in the "Cloud"?**

Yes, you can password protect a document stored in the "Cloud" but it will not protect the information. For example, do not store "sensitive personal" information in Googledocs or Dropbox. Anonymise data where possible. The College is currently investigating a solution to "Cloud" storage.

6. **What is the difference between password protection and encryption?**

Password protection protects a file but there are tools out there to run against files to crack Microsoft Office passwords. More recent versions of Office seem more secure though.

Encryption is the jumbling of data held in a file accessed by knowing the key which essentially is a password.

In disk encryption such as McAfee or Bitlocker the whole disk is encrypted, meaning if you moved the hard disk to another computer it would still be encrypted.

With file encryption such as 7zip or more recent versions of Office you can encrypt files, which should offer more resistance to attempts to crack into than just password protection.

7. What are the criteria for historical records retention – what information should be retained long-term?

The College's Records and Data Retention Schedule identifies vital and historically important records, which are suitable for transfer to the College Archives. The Schedule can be found at the following link: http://www.kcl.ac.uk/library/info-management/information/retention/index.aspx.

Alternatively, please contact the Information Management team (records-management@kcl.ac.uk) who'll be happy to carry out an appraisal of your records and provide retention advice.

8. Can we use data for a different purpose if it is anonymised?

Yes, if the data is truly anonymised it can be used for a different purpose as it is no longer considered personal data. It is important to note that any personal information the College holds will not cease to be personal data until the identifying dataset is securely disposed of and there is no means of recovering it.

9. Research funders such as the Medical Research Council asks researchers to retain data for long periods of time; is this ok in light of the requirements of Principle 5 of the DPA – personal information must not be retained for longer than is necessary?

Yes, it is ok as there are legal or business reasons for keeping the data. Not all information might need to be retained though; it would be appropriate to destroy any transitional data e.g. emails which are not recording a decision. Outlook is not a record-keeping system.

10. It would take too long to go through all of my emails to see which ones were relevant to retain....do you have any practical tips?

The Information Management team offer training on email management, either for individuals or teams. To book a session, please email records-management@kcl.ac.uk. We also have a factsheet on managing email at http://www.kcl.ac.uk/library/info-management/guidance/email.pdf.

11. What about data which has been anonymised but is still sensitive from a reputational point of view e.g. interview transcripts

It would be a good idea to encrypt any data which you believe is sensitive.

12. I find it difficult to remember passwords; do you have any tips?

There is software you can use which will store your passwords securely. For example KeePass - http://keepass.info/ .

13. For how long should CCTV footage be retained?

A new CCTV Policy is in the process of being approved and will be published in June 2012. The retention for CCTV footage in the Policy is no longer than 90 days from the date of recording, unless required for evidential purposes or the investigation of crime or otherwise required by law. At the end of their useful life all images on discs should be erased and securely disposed of as confidential waste. All still photographs and hard copy prints should also be securely disposed of as confidential waste.

14. If you are using a courier to transfer records; does the College have a preferred courier?

Yes, the College has a preferred courier. Please find details at the following link: http://www.kcl.ac.uk/about/structure/admin/purchasing/internal/peferred/couriers.html.

If you are sending personal or sensitive personal data via a courier you should check the conditions of carriage to see if Data Protection is referred to and if sensitive data is being transferred you should identify any specific requirements you need to be adhered to in a separate document and agree with the company.

15. Can I upload my KCL email account to my mobile phone or iPad?

If you are uploading KCL email to your mobile device you should ensure that it is encrypted. It is more secure to dial into the College's network than to hold emails on your mobile devices.

16. As a programme administrator, I receive hundreds of emails from students. How do I know which emails are 'core emails' and where should I store these?

Any emails relating to student entry, progression or outcome should be added to the student record. This may mean printing emails out and adding them to the paper student file. If your department has AKGD or a shared server, emails can be saved centrally so that they are accessible to all colleagues. These could be arranged by year and programme, with a folder for each student, to assist with searching and locating emails efficiently.

The Information Management team are currently working on a checklist of student emails which may have long term value. If you are interested in receiving a copy of this checklist once complete, please contact the team (records-management@kcl.ac.uk).

17. Is it necessary to weed paper student files prior to transfer to archive storage?

A factsheet on the recommended content of a paper student file is available on the Information Management web pages at http://www.kcl.ac.uk/library/info-management/guidance/checklist.pdf. It is recommended that administrators refer to this guidance and weed any records not identified on this list prior to transfer of files to storage.

It is recognised that student information is now increasingly being kept in hybrid format. It is acceptable for items on the checklist above to be held in electronic rather than paper format, i.e. on SITS or in databases.

18. Is it acceptable to scan documents rather than retain paper copies?

Generally scanning is acceptable, providing that sensible rules are followed. There have been examples of only one side of a double-sided document being scanned, which obviously causes problems if the original paper copy has been disposed of. There are also set scanning standards which should be adhered to, to ensure the quality of the image and admissibility in court. The Information Management team will be publishing guidance on this shortly. For further enquiries, please contact the team directly, email records-management@kcl.ac.uk.