Electronic Data Security

Information Commissioners Office www.ico.gov.uk

Network Security http://www.kcl.ac.uk/onespace/it/security/

Data Security http://www.kcl.ac.uk/onespace/it/security/data.html

Education http://www.getsafeonline.org/nqcontent.cfm?a_name=videos_1

(1) Should data be encrypted

Is the data is person identifying and could cause harm or distress to a living individual as per Legal Compliances. What may also help is referencing the Data Classification guide http://www.kcl.ac.uk/onespace/it/security/data.html and treating data as if it is about you. Anonymise data with key stored separately. Important data should always be backed up, if someone else does this for you verify it is being done and should be backed up to a safe network store or an encrypted location. Consider other types of data such as voice and video and the impact of placing on the web.

(2) Remote Access
- Remotely access data on a data store.
- Firepass.kcl.ac.uk, client for Windows, App for iPad, iPhone
- AKGD desktop.kcl.ac.uk

(3) Desktop / Laptop encryption
- McAfee Endpoint encryption for King's owned Windows machines with McAfee Agent installed. Not RAID. Not dual boot. Fill in McAfee encryption request form.
- Macintosh machines file vault encryption.
- Truecrypt for Windows, Mac and Linux is a free download to create a volume.
- Bitlocker for Windows 7 computers.

(4) Physical Security
- Locking equipment away in sensible place
- Kensington locks
- Mini macs, lock away?

(5) Removable storage
- Ironkey,4 gig FIPS 140-2 (AES 256), Uncheck option Contact head of School to contact ISS. While setting password select 'reset device' option initially and wipes if forget password.
- Non encrypted USB sticks can be encrypted with Truecrypt.
- Purchase encrypted external hard drives such as AES 256 Iomega drive. If have unencrypted external drive should be able to encrypt with Truecrypt.

(6) KCL Email
- Use Outlook web access http://www.kcl.ac.uk/iss/explore/access/owa.html and don't save passwords.
- transfer.kcl.ac.uk to transfer files.
- Encrypt files with 7zip, Winzip before emailing / transferring.

(7) Smart phones / iPad / Mobiles

- Blackberry: if owned by King's get the corporate encryption enabled. If not owned by King's turn on content protection.
- Iphones upgrade to 4.0 / 5.0 accept updates, and see guidance on web site. HTC etc see website.
- iPad follow guidance.
- Allow email? but must have a Pin, could configure to enable password at every connection to email? Could replace Pin with stronger password, turn on autolock, should log with www.me.com to allow remote formatting in case of loss.

(8) Data Destruction

- Delete files, empty recycle bin, only keep as long as needed.
- Boot and Nuke old desktops / laptops and refer to PC disposal procedures.

(9) Password Management

- http://keepass.info
- Reset passwords upon confirmed email from ITS see password policy or via Onespace and reset password.
- Do not use King's password elsewhere
- Do not register on remote websites using

(10) Malware

- McAfee ePo www.kcl.ac.uk/antivirus
- McAfee for non Microsoft
- Microsoft Security Essentials
- ClamXAV / Sophos / Avast free for Mac at home
- Malwarebytes on home machines
- Microsoft System Sweep

(11)Recent relevant policies on Policy Zone on Google

- Outsourcing data
- Data loss reporting procedure
- Sharing personal data
- Mobile device policy

(12) Firewalls

- Turn it on if off

(13) Software patching

- Windows updates
- Macintosh updates
- Microsoft Baseline Analyser