Code of practice 6 - Security of laptops and the data stored therein

1. Introduction

The use of laptops and other electronic computing devices [1] is commonplace these days as the need to record, store, process and transmit data electronically increases, as well as the ability to work away from the office. The fact that these devices are portable means that they can be carried off College premises and can be connected to more than one network. As a result, they are more likely to be lost or misplaced and the data they contain fall into the hands of unauthorised persons. Such breaches of security could have severe consequences for the College, in the loss of highly important commercial data, for the individual, in the loss of vital research data, or from the unauthorised disclosure of sensitive personal data. It could possibly lead to legal proceedings being taken against the Data Owner and/or the College.

Any individual connecting a laptop to the College network automatically renders the use of that device subject to College rules, irrespective of whether or not it is being used to process College-related data.

Individuals who use a laptop to process College-related data must do all that is reasonable to keep their laptop, associated media and the data contained therein secure at all times.

Data should not be carried on a laptop unless a risk assessment has been carried out beforehand and appropriate risk management processes put in place.

2. Authorisation

You may use laptops to process data as part of your employment as a member of staff, as an honorary member of staff or as a registered student, if authorised to do so by the Head of your College Administrative Unit (CAU) or by his/her nominated representative. In the case of students this will normally be that student's supervisor. This authorisation will normally be effected through the Department's Information Systems Liaison Officer who should ensure that the owner of the laptop is made aware of the encryption tools available for securing the data to be held. Additionally, authorisation must be given before staff and students are permitted to carry College-related data away from College premises and process them off-site.

3. Security of data held within the device or on associated media

3.1 Data must not be carried on laptops unless that data is adequately secured. A risk assessment must be carried out [2] and appropriate risk management procedures determined and put into place before data is put on to a laptop and prior to leaving the College or leaving an authorised off-site location and returning to the College. The level of security required will depend upon the sensitivity of that data, for example sensitive personal data, valuable commercial data, research data that cannot be easily replicated or may have patent potential will all require high levels of security. Hence, encryption of the device's disk may need to be carried out so that if, in spite of taking measures to ensure the security of the device, it falls into the wrong hands, the data cannot be accessed by unauthorised personnel. All laptops must have an up-to-date virus scanning programme installed.

3.2 When processing personal data on laptops you must take all reasonable steps to ensure the security of that personal data. This is one of the eight Data Protection Principles set out in the Data Protection Act 1998 and the College Data Protection Policy [3] with which you must comply. In particular, when using a laptop, you must not process personal data in public places e.g. when travelling on public transport. All processing should be carried out in privacy, even within your own home, to avoid accidental disclosure to non-authorised persons. It is an offence to deliberately disclose personal data
to an unauthorised person. As with commercially sensitive data, a risk assessment should be carried out and the appropriate procedures put in place. This may involve encryption, anonymisation of the data or key coding, with the key code being kept securely and separately.

3.3 Sensitive personal data, as defined in the Act, should not be stored in these systems unless you can demonstrate that you have taken special security precautions e.g. encryption of files on the hard disk or on a storage medium (College Data Protection Policy refers [4]). In addition, such data should be processed on this system or on a network only where you have registered the processing activity with your Departmental Data Protection Co-ordinator.

3.4 When processing patient data, you should note that the Hospital Trusts each have their own policy regarding the use of laptops for storing and processing of patient data. Members of staff and students must ensure that they comply with the relevant Trust policy before processing any patient data owned by a Trust on such a device.

4. Security of a laptop and associated media

When laptops are used to record, store, process or transmit data as part of your employment as a member of staff or your registration as a student, you should take such measures as are appropriate to ensure the security of the device, in accordance with the College Information Systems Policy and associated codes of good practice [www.imperial.ac.uk/ict/security refers]. Because of their portable nature you should keep laptops in a locked brief case or similar container and these containers should not be left unattended during the course of your journey, nor should they be left exposed on the seat of a car or other vehicle. Always protect access to your laptop by using a system password, if at all possible. Whilst this will not provide complete security, it will often prevent casual interception of the data, for example, in some cases of loss or theft. You should be aware that anyone stealing or finding a laptop could use it to gain access to the College network and do untold damage not only to your data but that of many others.

5. Connection to the college network

You may only connect your laptop to the College network when you have been authorised to do so and then you should do so in accordance with College Information Systems Security Policy. If your laptop stores sensitive data you should ensure that you connect it to the College network for as short a time as possible, commensurate with the processing in hand. Once a laptop is connected to the network it is possible to access data held on other devices or networks. In addition, you should not allow any other person to access the network from your laptop by using your login/password or by giving them your login/password to use with their own laptop.

Laptops attached to the College network will be treated just the same as any other computing system connected to the network. Hence, for example, you should not use or attempt to use such a device to transmit pornographic material or to harass or libel others. Nor should you store such material on a laptop used, even in part, for College business. Such actions are illegal and will lead disciplinary action being taken by the College and possibly to criminal and/or civil proceedings being taken against you.