Mobile Computing Policy

Overview and Scope

1. The purpose of this policy is to ensure that effective measures are in place to protect against the risks of using mobile computing and communication facilities. . However, the policy applies equally to information stored on or accessed via home PCs.

2. All users must adhere to this policy. Users in breach of this policy will be liable to disciplinary action under University procedures.

3. If you are unsure whether any of your computing activity may breach University policies, you should seek advice before proceeding. You can contact Information Services for advice by emailing infosec@qub.ac.uk).

4. Users should read this policy in conjunction with the *Computer Resources - Acceptable Use Policy*, and Regulations and Statements of Best Practice relating to Information Security and Information Handling available at http://go.qub.ac.uk/itpolicies. Changes to this policy in response to changing demand, both operational and legislative, will be available on the University WWW site.

Information Handling

5. The University's Information Handling Policy (available at: http://go.qub.ac.uk/itpolicies) sets out the minimum standards that must be adhered to when handling sensitive information. Those standards apply equally when handling sensitive information on mobile devices.

Working Off-Site

6. The physical and logical controls that are available within the University environment are not automatically available when working outside of that environment. There is an increased risk of information being subject to loss or unauthorised access. Mobile computing users must take special measures to protect sensitive information in these circumstances

7. Removal off-site of the University's information assets, on laptops or other mobile devices, must be properly authorised by the responsible information owner. Prior to authorisation a risk assessment should be carried out, to protect against loss or unauthorised access, and appropriate risk management processes put in place. The risk assessment must take into account the sensitivity of the information. A risk assessment template is attached to this policy.

8. Staff accessing information systems remotely to support business activities (including from home PCs) must be authorised to do so by the responsible information owner. Prior to authorisation a **risk assessment** should be carried out and appropriate risk management processes put in place. The risk assessment must take into account the **sensitivity** of the information.

9. Laptops and home personal computers should not be used for business activities without **appropriate security measures**, including up to date security "patches" and virus protection (see http://go.qub.ac.uk/itpolicies).

10. When undertaking mobile computing the following guidelines must be followed:
    a. When travelling, equipment (and media) must not be left unattended in public places. Portable computers should be carried as hand luggage when travelling.
    b. When using a laptop, do not process personal or sensitive data in public places e.g. on public transport.
    c. Passwords or other access tokens for access to the University's systems should never be stored on mobile devices where they may be stolen or permit unauthorised access to information assets. For example, options to automatically "remember" passwords should not be accepted. Passwords and passkeys should not be saved on the mobile device.
    d. Security risks (e.g. of damage, theft) may vary considerably between locations and this should be taken into account when determining the most appropriate security measures.

11. When working with other organisations (e.g. NHS), make sure that you comply with their guidelines relating to mobile computing.

Wireless and Non-University Networks

12. As part of the risk assessments described above, information owners and mobile users must take account of the risks associated with using **wireless networks and non-University networks**. The University's Information Handling Policy stipulates that sensitive data or information may only be transferred across networks when the confidentiality of the data or information can be assured throughout the transfer. The following should be noted:
    a. Wireless networks and public networks are less secure than the University's private, wired network environment.

b. Email is an inherently unsecure way of transferring sensitive information and should be used with caution.
c. Where there is no alternative to transferring/accessing sensitive information across unsecure networks or by email, advice should be sought on appropriate steps to protect the information. Information Services and School-based Computing Officers will advise on appropriate mechanisms for the secure transfer of sensitive information, particularly outside of the University's secure environment.

Laptops and Mobile Devices

13. Sensitive data stored on laptops and other mobile devices should be **kept to a minimum** to reduce risk and impact should a breach of security occur.

14. **Loss** of any mobile device containing sensitive data, or any other security breach, must be reported immediately to Information Services (**infosec@qub.ac.uk**) and Queen's Security.

15. Sensitive information held on any mobile device must be securely erased before the device is reassigned to another user or to another purpose. Where necessary, advice should be sought from Information Services and School-based Computing Officers on appropriate tools for erasing information on PCs and mobile devices.

16. USB memory sticks are prone to loss or theft. Add-on encryption to these devices can be left turned off. The product recommended by the University is the **IronKey**. This has inbuilt encryption which cannot be turned off, is resistant to physical disassembly and destroys the data after 10 failed attempts to access. These devices will be supplied through the Computer Shop in The McClay Library.

17. Mobile devices are vulnerable to theft, loss or unauthorised access when taken outside of the University's physical environment. They must be provided with appropriate forms of access protection to prevent unauthorised access to their contents:
    a. Password protection must be in place, while recognising that passwords offer only limited protection against a determined attack.
    b. Time-out protection (e.g. screen saver or hibernation with password) must be applied.
    c. Where sensitive information is held on laptops or mobile storage devices, data encryption must be applied to that information or to the entire device.
    d. The mandated system for data encryption on laptop devices is Truecrypt (see http://www.qub.ac.uk/directorates/InformationServices/Services/Security/Encryption/).
    e. Full device offers the maximum protection for sensitive information on laptops and other devices and should be used where the sensitivity of

data requires it. Alternatively and where appropriate, data can be encrypted at the partition level or virtual partition (a file encrypted to behave like a disk partition) level. In most cases, encrypted virtual partitions or disks can be copied to USB pens, CDs and DVDs for safe transportation.

f. Note that data is only protected by encryption when the laptop is powered off and not in normal use.
g. Access to encrypted information is lost if the encryption key is forgotten. Users should ensure that a secure, unencrypted backup copy of encrypted information is retained on central systems.
h. Information Services and School-based Computing Officers will offer advice on encryption products, options and configuration.

Information Asset		**Information Owner**	
Description of Information Handling Requirement			

Description of Risk	**Impact** **1. Minor** **2. Moderate** **3. Significant**		**Likelihood** **1. Low** **2. Moderate** **3. High** **4. Very High**		**Impact * Likelihood**		**Action to reduce risk**	**Respon-sibility**
	Gross	Net	Gross	Net	Gross	Net		