Information Security Policy

Overview and Scope

1. The purpose of the Policy is to protect the University's information assets from all threats, whether internal or external, deliberate or accidental. Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on mobile or removable devices, or spoken in conversations or over the telephone.

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 University policies on *Computer Resources - Acceptable Use, Mobile Computing, Information Handling* and *Passwords* 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 website.

Information Security

5. It is the Policy of the University to use all reasonably practicable measures to ensure that:
    a. Information will be protected against unauthorised access.
    b. Confidentiality of information is assured including the protection of information from unauthorised disclosure or intelligible interruption.
    c. Integrity of information is maintained including safeguarding the accuracy and completeness of information by protecting against unauthorised modification.
    d. Regulatory and legislative requirements will be met. This applies to record keeping and most controls will already be in place; it includes the requirements of legislation such as the Companies Act and the Data Protection Act.

e. Business Continuity plans will be produced, maintained and tested to ensure that information and vital services are available to users when they need them.
f. University requirements for availability of information and information systems will be met.

6. All academic and academic support managers are directly responsible for implementing the Policy within their business areas, and for adherence by their staff.

7. It is the responsibility of each employee to do everything reasonable within their power to ensure that the University Policy is carried into effect.

8. Staff should report breaches of information security, actual or suspected, to their line manager or, if that is not possible, to the Director of Information Services. Students should report breaches of information security, actual or suspected, to their Head of School or, if that is not possible, to the Dean of the relevant Faculty. Students in the Student Computing Areas (SCAs) or similar computing facilities may report breaches of information security, actual or suspected, to the centre supervisor. Staff and students should report more general security incidents or threats either to the appropriate person identified above or directly to Information Services by emailing infosec@qub.ac.uk . Breaches of the security policies will be investigated in accordance with the University's disciplinary procedures.