QUB Information Security Policy

Version	Date	Changes	Author	Approver
1.0 Approved	4th December 2024	Updated following review	James Vincent (Cyber Security Manager)	Greg McCloskey (Director of D&IS)

Introduction

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.

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

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

Users should read this policy in conjunction with the university policies on Computer Resources - Acceptable Use, Mobile Computing, Information Handling, Passwords and any other policy available at https://www.qub.ac.uk/directorates/InformationServices/Services/Security/Gen-Policies/ . Changes to this policy in response to changing demand, both operational and legislative, will be available on the University website.

Policy Objectives:

This policy exists to ensure that all reasonably practicable measures are in place 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.

Scope:

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

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

Compliance:

All staff members are expected to comply with this policy.

Policy Review:

This policy will be reviewed bi-annually (as a minimum) to ensure that it remains current and effective in meeting the organisation's security and accessibility needs.