



STRANMILLIS UNIVERSITY COLLEGE

A College of Queen's University Belfast

Information security policy statement

OBJECTIVE

The objective of **information** security is to ensure business continuity by **preventing** breaches of security.

Notes

1 *Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes and diskettes, or spoken in conversations or over the telephone.*

2 *The protection of information from unauthorised disclosure or intelligible interruption.*

3 *Safeguarding the accuracy and completeness of information by protecting against unauthorised modification.*

4 *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.*

5 *To ensure that information and vital services are available to users when they need them*

POLICY

➤ The purpose of the Policy is to **protect the University College's information assets**¹ from **all** threats, whether internal or external, deliberate or accidental.

➤ It is the Policy of the University College to use all reasonably practicable measures to ensure that:

➤ Information will be **protected against unauthorised access**.

➤ **Confidentiality** of information is assured.²

➤ **Integrity** of information is maintained.³

➤ **Regulatory and legislative** requirements will be met.⁴

➤ **Business Continuity plans** will be produced, maintained and tested.⁵

➤ University College requirements **for availability of information and information systems** will be met.

➤ This statement should be read in conjunction with the University College's Regulations relating to:-

➤ Regulations for Acceptable Use of IT Systems

➤ Data Protection

➤ All academic and support staff 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 College's Policy is carried into effect.

➤ It is the responsibility of employees to safeguard their system password. Passwords must not be written down in obvious locations or divulged to third parties. Also passwords, which are easy to guess, must not be used and passwords chosen for University College systems must not be used for other purposes.

➤ Breaches of information security, actual or suspected, should be reported to the *IT Services Manager*, who will, if appropriate, inform the relevant person, under the relevant Disciplinary Procedure.

➤ Changes to this policy in response to changing demand, both operational and legislative, will be available on the University College's website.
