INFORMATION SECURITY POLICY

Purpose & Scope

This Information Security Policy is relevant to all curriculum and support areas and to all of the staff within them.

It is the policy of the College to ensure that the information it manages is appropriately secreted to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of information.

This policy provides management direction and support for information security across all support areas and departments and is intended to serve as an overarching policy, relating to a number of other policies listed below. These specific policies are considered to be part of the Information Security Policy and will have equal standing.

Information managed by the College is not just held in electronic format and therefore this Policy covers the security of information held on all media.

Policy Statement

Responsibility for ensuring compliance with this Policy lies with the Senior Leadership Team.
The Senior Information Risk Owner for the college is the Principal & Chief Executive. The SIRO is responsible for ensuring information security risk assessments are completed, policy breaches are addressed and acts as advocate for information risk management at the highest level.

The Computer Systems department is responsible for the maintenance of this Policy as well as maintaining associated guidelines and promoting compliance with them.

Compliance with this Policy and any associated procedures is compulsory for all staff employed by the College. A member of staff who fails to comply with the Policy may be subjected to disciplinary action under the College Disciplinary Policy. It is the responsibility of the full Management Team to ensure that staff are aware of the existence of this Policy and its content.
This Policy also consists of a number of more specific policies, these are:
IT Acceptable Use Policy, Data Protection Policy, Secure Network Access Policy and the Business Continuity Plan.

This Policy follows the JISC UCISA Information Security Toolkit (edition 2.0) and includes links to a number of college policies, procedures and guidelines. The College will maintain its Cyber Essentials compliance as well as working towards Cyber Essentials Plus and ISO 27001 Information Security Management compliance. Compliance with this Policy with other information related legislation, including the Data Protection Act 2018.

The Senior Leadership Team (SLT) will ensure that there is clear direction, adequate resourcing and visible management support for security initiatives.
The Computer Systems will devise and coordinate the implementation of information security controls according to this Policy. The Department will also advice the management team on any risk management issues arising from the implementation of new systems.
The responsibility for ensuring the protection of information systems and ensuring that specific security processes are carried out will lie with the security owner.

New information systems will be identified and authorised by the Vice Principal, Resources with support from the Data Protection Officer (Director of Finance and Funding) and IT Manager. To determine the appropriate levels of security measures applied to information systems, a process of risk assessment will be carried out for each system to identify the probability and impact of security failures. Where Personal Data is held in a system a Privacy Impact Assessment must also be carried

out. Usually, the System Owner will carry out these assessments in consultation with relevant members of the Computer Systems department.

The risk posed to the College by potential failures in the security of information held in paper or manual systems will also be considered under this Policy. Responsibility for these assessments will lie with the head of the department managing the information.

The College will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies and network and telecommunications operators in respect of this policy.

This policy has been reviewed regarding the requirement for an Equality and Diversity Impact Assessment and a Privacy Impact Assessment.
At this stage it is felt that a full impact or privacy assessment is unnecessary as the college public duty has been discharged through a related policy/procedure or there is no current requirement

Document Control		**Linked Policies/Strategies**	**Linked Procedures**
Policy	Information Security	IT Acceptable Use Policy Data Protection Policy Secure Network Access Policy	Business Continuity Plan
Responsibility	VP Resources		
Approval Date	August 25		
Review Date	August 27		
Approval Group	SLT		