



Information Management Policy

May 2017 (May 2018)

This policy applies to :	All employees, temporary staff, contractual third parties, partners or agents of the college who have access to any information systems or information for college purposes.
Author/Department:	Business Support Manager
Area/Person responsible:	Principal
Date approved:	25/05/2017
Related Documents/ Policies:	Data Protection and Freedom of Information Policy, Staff Acceptable Use Policy (ICT), Student Acceptable Use Policy (ICT), Information Management Guidance and Procedures
Date of Next Review:	01/05/2019

Date of most recent review:	01/05/2018
Changes made:	Reviewed and references made to new legislation.

The Equality Act 2010: The Equality Duty

The College has a duty to consider the needs of all individuals in our day-to-day work – in shaping policy, in delivering services and in relation to our employees. The Equality Duty has three aims, which require the College to have due regard to the need to:

- **Eliminate unlawful discrimination**, harassment, victimisation and any other conduct prohibited by the Act;
- **Advance equality of opportunity** between people who share a protected characteristic and people who do not share it; and
- **Foster good relations** between people who share a protected characteristic and people who do not share it.

Does the policy support the aims of the Equality Duty?	Yes	X	No		N/A	
If no, please state which groups may be affected and complete a full equalities impact assessment (guidance and forms available on the intranet)						
Impact Assessment Reference:						

Initial Impact Assessment Completed	
Review of Policy	

Date	
Date	

1 Introduction

- 1.1. Information is a valuable asset that the College has a duty and responsibility to protect. This responsibility is placed on the College by the EU General Data Protection Regulations (GDPR) and the Data Protection Act 2018, monitored and regulated by the Information Commissioner's Office.
- 1.2. The College recognises that by efficiently, effectively and ethically managing its information, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Information recorded provides evidence for protecting the legal rights and interests of the college, and evidence for demonstrating performance and accountability.
- 1.3. The College is committed to protecting the security of data through the preservation of:
 - **Confidentiality:** protecting information from unauthorised access and disclosure
 - **Integrity:** safeguarding the accuracy and completeness of information and processing methods.
 - **Availability:** ensuring that information and associated services are available to authorised users when required.
- 1.4. To support this commitment, the College has developed an Information Management Framework, the core of which is this document which provides the policy framework through which this effective management can be achieved and audited. It covers:
 - Scope
 - Responsibilities
 - Relationships with existing Policies.

2 Scope of the policy

- 2.1. This policy applies to all information in all forms including, but not limited to:
 - Hard copy or documents printed or written on paper;
 - Information or data stored electronically, including scanned images;
 - Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
 - Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
 - Information stored on portable computing devices including mobile telephones, PDA's and laptops;
 - Speech, voice recordings and verbal communications, including voicemail; and
 - Published web content, for example intranet, internet and social media.

3 Responsibilities

- 3.1. The college has a corporate responsibility to maintain its recorded information and information management systems in accordance with the regulatory environment with the overriding objective to keep the college's information safe. The person with overall responsibility for this policy is the Principal.
- 3.2. The Business Support Manger will give guidance on good information management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if information is stored securely and can be accessed appropriately.

- 3.3. Members of the Senior Leadership Team, Heads of Department and Support Managers have the responsibility and accountability for managing the risks within their own work areas.
- 3.4. Individual staff and employees must ensure that recorded information for which they are responsible is accurate and is maintained and disposed of in accordance with the college's information management guidelines as set out in the Information Management Guidance and Procedures.

4 Relationship with existing policies/guidance

- 4.1. This policy has been drawn up within the context of:
 - a. Information Management Framework
 - b. Information Charter
 - c. Data Protection and Freedom of Information Policy
 - d. Information Management Guidance and Procedures
 - e. Retention and Disposal Guidance and Schedule
 - f. Staff Acceptable Use Policy (ICT)
 - g. Student Acceptable Use Policy (ICT)
 - h. Other legislation or regulations (including audit, equal opportunities and ethics) affecting the college.