

## Social Media Policy

### 1.0 Policy Statement

1.1 The College recognises that the internet provides unique opportunities to participate in interactive discussions, engage with the wider community, and share information on particular topics using a wide variety of social media, such as Facebook, Twitter, blogs and wikis. However, employees' use of social media can pose risks to the College's confidential and proprietary information, and reputation, and can jeopardise the College's compliance with legal obligations.

1.2 To minimise these risks, to avoid loss of productivity and to ensure that the College's IT resources are not compromised, this Policy, which is a part of any other policies recognised by the College, and any other policies recognised by the College, be amended at any time by the College.

1.4 Nothing in this Policy is intended to restrict or undermine the right to academic freedom.

### 2.0 Who is covered by the policy

2.1 This policy covers all individuals working at all levels as to the College's electronic communication systems and equipment required to comply with this policy.

### 3.0 Scope and purpose of the policy

3.1

- 3.3 The purpose of this policy is to encourage good practice; to protect the College, its staff and students; to clarify where and how existing policies and procedures apply to social media and to promote effective and innovative use of social media as part of the College's activities.
- 3.4 Breach of this policy may result in disciplinary action up to

of my employer". Employees should also ensure that their profile and any content they post are consistent with the professional image they present to students, clients, and colleagues.

- (e) Staff should avoid posting comments about sensitive business-related topics, such as (m)0.5(m)TJ 0.003 Tc -0

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the Head of IT Infrastructure Services.

- 5.2 All managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.
- 5.3 All staff are responsible for the effectiveness of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the Head of IT Infrastructure Services or Human Resources. Questions regarding the content or application of this policy should be directed to the Head of IT Infrastructure Services or Human Resources.
- 6.0 Compliance with related policies and agreements
- 6.1 Social media should never be used in a way that breaches any of the College's other policies. If an internet post would breach any of the College's policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to: rnet

0.711 0 Td 0 Td ( )Tj a)24 0 Td (i)Tj 0.78i



- 9.3 The College may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.
- 9.4 Staff should not use the College's IT resources and communications systems for any matter that they wish to be kept private or confidential from the College.
- 9.5 For further information, please refer to the College's IT Acceptable Use Policy.
- 10.0 Monitoring and review of this policy
- 10.1 The Information Security Group (ISG) in conjunction with the IT Strategy Working Group (ITSWG) shall be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice.