# SOCIAL MEDIA POLICY

This policy is available on-line at: www.tynecoast.ac.uk

- We will consider any request for this policy to be made available in an alternative format or language. Please note that the College may charge for this. Please contact: Director of IT.
- We review our policies regularly to update them and to ensure that they are accessible and fair to all. We welcome suggestions for improving the accessibility or fairness of this policy.
- All our policies are subject to equality impact assessments*. We are always keen to hear from anyone who wishes to contribute to these impact assessments. Please contact: Director of IT.

*Equality Impact Assessments are carried out to see whether the policy has, or is likely to have, a negative impact on grounds of: age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex or sexual orientation

| Approved by: | Version: | Issue Date: | Review Date: | Contact Person: |
|---|---|---|---|---|
| SEG, JCC | v.3 | Jan 2021 | Jan 2024 | Director of IT |

**Equal Opportunities:** **Impact Assessed**

**Review:** **3 years**

**POLICY NUMBER 82**

# SOCIAL MEDIA POLICY

## 1. Policy Statement

The use of social media is widespread in our society, both for personal and business purposes. Social media presents unprecedented communications opportunities and risks.

The College wishes to encourage the safe and responsible use of social media as part of its teaching & learning and business support provisions. The purpose of this policy is to minimise the risk to the College through this use.

## 2. Scope

This Policy applies to all social media services or applications used by employees or contractors.

Social Media/Networking is defined as a website, service or other application which enables users to communicate with each other by posting/sharing information, comments, messages, images, videos etc. This therefore includes, but is not limited to, Facebook, LinkedIn, Twitter, Wikipedia, Instagram, Tick Tock and all other social networking sites, internet postings and blogs.

## 3. Legislation

- Data Protection Act 2018
- Computer Misuse Act 1990
- Copyright Designs & Patents Act 1988
- Malicious Communication Act 1998

## 4. Responsibilities

Everyone has a responsibility to give full and active support for the Policy by ensuring:

4.1. The Policy is known, understood and implemented
4.2. Behaviour not in accord with the Policy is challenged.

Within this general responsibility there are some specific responsibilities:

4.3. The Director of IT, for the effective implementation of the Policy.
4.4. The Head of Marketing for the monitoring of authorised social media accounts

## 5. Actions to Implement and Develop Policy

5.1. Use for Business Purposes

5.1.1. Authorisation

Approval should be obtained from the Marketing department prior to creating any social media accounts or groups that will be used for business purposes.

Business purposes include, but are not limited to:

- Promotion of departments/facilities
- Promotion of events
- Communication with learners
- Learner discussion groups

5.1.2. Credentials

Any social media accounts created for business purposes should be setup using an official "@tynecoast.ac.uk" or other approved accounts, e.g @stc.ac.uk e-mail address. IT Services can, if required provide accounts to be used for this purpose.

The Marketing department should be informed of the internet address and username/password that can be used to access the account.

If contacted for comments about the College for publication anywhere, including in any social media outlet, users should direct the enquiry to the Marketing department and not respond without written approval.

5.2. Personal Use

Occasional personal use of social media during working hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and complies with this policy. Personal use is a privilege and not a right. It must not be overused or abused. The College may withdraw permission for it at any time or restrict access at its discretion

5.3. Acceptance of Friends

Social media is used by many people to communicate with their peers and the public. Learners may wish to form personal relationships with employees. In the interests of ensuring professional boundaries are maintained employees must not become friends with, add to their social media network or otherwise communicate with any potential students (applicants), current students, former students under the age of 19 or parents unless a clear reason exists, for example, the student is a relative or family friend.

Entering into such a relationship may lead to abuse of an employee's position of trust and breach the standards of professional behaviour and conduct expected by the College.

5.4. Prohibited use

Users must not use social media in either work or personal time to:

- Make statements that could be deemed to be defamatory, offensive, obscene, abusive, proprietary, or libellous

- Make statements that would contravene this, or any other College policy.
- Discuss students or co-workers or publicly criticise College polices or personnel
- Post images or videos that include learners on social networking sites
- List their College e-mail address "@stc.ac.uk" as a contact address for personal social network accounts, other than those aimed specifically at the professional market and used for networking and career development, such as LinkedIn
- Misrepresent the College's interests, whether these interests are in the public domain or not.
- Act, without permission, as a spokesperson for the College.
- Carry out any action which adversely affects the College's reputation or undermines its core business or related interests.
- Publish information that would be in breach of the Data Protection or Information Security polices
- Staff and learners should not create pages, sections, news groups or equivalent on social networking services that claim to be linked to or represent the College without authorisation from the Marketing department
- Misappropriate or infringe the intellectual property of other organisations and individuals.

All staff should assume that their contributions on social media will be associated with the College's business and also seen and read by other members of staff.

5.5. Guidelines

When making use of social media users are advised to:

- Review the security and privacy settings on all social networking services they use. We recommend that all privacy settings be set to "only friends". "Friends of Friends" will allow anyone who is a friend of any of your friends to see your profile, photos of you, comments you have posted etc.
- Be respectful to others when making any statement on social media and be aware that they are personally responsible for all communications which will be published on the internet for people to see.
- Consider the appropriate use of social media/networks to ensure that the safeguarding of students is maintained at all times.
- Ensure any publically visible (or potentially publically visible) activity on social media/networking sites reflects the College's core values and principles and that their profile and content posted is consistent with the professional image presented to colleagues and students.
- Make it clear in social media postings, or in their personal profile, that they are speaking on their own behalf and not on behalf of the College, for example by labelling their entry as "views are my own and do not represent those of my employer"

5.6. Social Media during recruitment and selection

The College will only view relevant social media websites as part of the pre-employment process, i.e. those aimed at specifically at the professional market and used for networking and career development, such as LinkedIn.

6. Monitoring

The College reserves the right to monitor, log and access internet access with or without notice, to or from any device owned by the College, or connected to the College's IT Systems to ensure this policy is being complied with.

The Marketing team will regularly review social media sites/accounts that are used for business purposes to ensure their usage complies with this Policy.

7. Consequences of failure to comply with legislation or policies

If a user fails to comply with the provisions outlined in this document, their access to IT Systems may be withdrawn and future access may be restricted. This may affect the individual's ability to undertake the duties of their job or continue their studies.

Serious or consistent non-compliance with this policy may be considered to be a disciplinary offence and will be dealt with in accordance with the College's disciplinary procedures or other appropriate action may be considered.

Acts of a criminal nature, or any safeguarding concerns may be referred to the police, Local Safeguarding Children Board (LSCB) and other relevant agencies.

## 8. Related Policies

- Harassment and Bullying Policy
- Data Protection Policy
- Information Security Policy
- E-Safety Policy
- Acceptable Use of IT
- Staff Disciplinary Procedure and Policy