Social Media Policy for Staff

Responsibility of: IT Services
Approval Date: January 2019
Review Date: January 2020
Approved By: Vice-Chancellor’s Executive
Section 1: Introduction, Purpose, Definition, and Scope

1.1 Social media platforms offer powerful new ways to express and share ideas. Their use presents the University and its staff with new and exciting opportunities; but it also introduces potential risks that must be managed.

1.2 The purpose of this policy is to protect the University’s students, staff, reputation, and values while supporting the effective use of social media to benefit the work of the University.

1.3 In this policy the term social media is used to describe a broad range of technology platforms which allow the creation and sharing of content across a virtual community. Examples include well known services such as Facebook, Twitter, LinkedIn, YouTube, Instagram, WhatsApp, and Snapchat; as well as smaller services such as personal blogs and discussion forums.

1.4 This policy applies to all staff, including individuals who have an honorary contract with the University, temporary workers, agency staff, and individuals engaged with the University on a self-employed contract basis.

Section 2: General principles

2.1 Staff must never use their personal social media to engage with students. For example, staff should never send a “friend” request to a student on Facebook, nor accept such a request from a student, and staff should never chat with students over WhatsApp or via Twitter direct message (DM).

2.2 Use of social media must at all times be consistent with other University policies, such as the Acceptable Use of Information Assets policy, the Data Protection policy, the Staff Student Relationship policy, and the Information Security policy. In particular, the University Code of Practice on Freedom of Speech applies to speech expressed via social media. Staff should also ensure that where they are teaching students under 18 that any communications with students is in line with the University’s Safeguarding Policy.

2.3 In order to protect the University’s students, staff, reputation, and values, care must be taken:

**NOT to breach confidentiality**, for example by:

- Revealing confidential University information.
- Revealing confidential University intellectual property.
- Revealing confidential information about an individual or organisation.

**NOT to do anything that could be considered discriminatory against, or bullying or harassment of, any individual**, for example by:

- Making offensive or derogatory comments relating to sex, race, gender, gender reassignment, race, nationality, religion or belief, disability, sexual orientation, or age.
- Using social media to bully an individual.
- Posting content or links to content that is discriminatory or offensive.

**NOT to breach copyright or other intellectual property laws**, for example by:

- Using other people’s images or written content without permission.

• Failing to give acknowledgement where permission has been given to reproduce something.

**NOT to bring the University into disrepute**, for example by:

• Unreasonably criticising or arguing with students, customers, colleagues, external stakeholders or competitors.
• Making defamatory comments about individuals or other groups.
• Posting inappropriate images or links to inappropriate content.

### Section 3: Official University social media accounts.

3.1 Members of staff can contribute to the social media activities of the University by writing for blogs, contributing content to official University social media accounts, or by helping with the running of official University social media accounts.

3.2 When contributing to the University’s social media activities you are representing the university and must at all times follow the published guidelines for use of official University social media.

3.3 If you wish to set-up a new official University social media account, you should in the first instance discuss with the Marketing team. Final approval for the creation of new official University social media accounts must be given by the Head of Marketing and Communications.

### Section 4: Using personal social media accounts

4.1 Social Media can be an effective way for staff to connect with peers in the University and in the wider world, to develop and improve their professional profile, and to support their work by providing opportunities for reflection, discovery, and collaboration. Staff are encouraged to do this, and to state and celebrate their connection with the University.

4.2 As a member of staff your activity on social media is likely to be associated with the University, regardless of whether you are acting in a professional or personal capacity, and whether you are using a using an official University social media account or a personal one.

4.3 Therefore when using a personal account in a professional capacity it is important to make it clear that you are acting on behalf of yourself and not the University. In particular:

- Do **not** use account names that suggest the account is an official UWL account.
- Do **not** use the UWL logo without official authorisation.
- Where your personal social media account indicates your association with the University, consider including a disclaimer such as “The views I express here are my own and not the views of the University of West London.”

4.4 Staff should ensure there is always a clear separation between work use and social use of their social media accounts.

### Section 5: Social media and teaching
5.1 The University provides a number of collaborative tools that are available to all, including Teams, Skype for Business, CampusPress, and Blackboard. Staff are encouraged to make use of these tools whenever possible.

5.2 Students may decide they wish to use their own personal social media accounts and tools for collaboration. Staff should not participate in or engage with such private groups, and students must not be encouraged or required to join them.

**Section 6: Monitoring and acceptable use**

6.1 The University reserves the right to monitor employees’ internet usage in accordance with the principles of information security. Valid reasons for checking an employee’s internet usage include suspicions that they employee has:
- • Been spending an excessive amount of time using social media websites for non-work-related activity; or
- • Acted in a way that is in breach of University policy.

**Section 7: Online Safety**

7.1 To protect yourself online, follow these key guidelines:

**Limit the personal information you post on social media.**
- Publish as little personal information as you can.
- Remember that it is often possible to link your individual social media accounts and so build up a wider picture of your social media footprint. So as well as considering how much personal information you publish on any single site, consider how much personal information you have published across all sites.
- Never publish your address or financial details on social media.
- Be aware of location services accidentally giving away personal information. Some social media platforms include your location with every new post. Posting from a mobile phone, in particular may include a precise GPS location. Smartphones and many cameras may also embed location data in digital photographs.
- Avoid allowing social media apps access to your contacts list or address book – in general, don’t give them information they don’t need.

**Watch out for fraud**
- Use the same caution when clicking links or opening documents from social media that you would for emails - social media is increasingly being targeted by phishers and other fraudsters.

**Keep your credentials safe**
- Beware of attempts to hijack your social media credentials. In particular, never log onto a social media account if prompted to after clicking a link in an email. Always go directly to the social media website in your browser.
- Use a strong, unique password for your social media accounts, and consider turning on two-factor authentication if it is available.

**Read the small print**
- Read the terms and conditions of social media services.
• In particular, for sites where you might publish original content such as photographs, make sure you understand what rights you are giving them to that content.

Be aware of the potential audience.

• Social media posts can be around for a long time, seen by more people than you expect, and subject to Freedom of Information (FOI) and data protection Subject Access Request (SAR) disclosure requests.
• So don't post anything on social media that you wouldn’t want widely seen - by colleagues, future employers, people you mention in the post, the press, or even the courts.

7.2 For more advice on keeping safe online, visit https://it.uwl.ac.uk/infosec

Section 8: Social media and recruitment

8.1 Social media sites such as LinkedIn can be an excellent source of leads for possible recruitment. However, when evaluating a candidate you should only look at their social media footprint where it is specifically relevant to their skills. Other searches or enquiries online should be used with caution, if needed at all, in order to ensure that the selection process is free from any unintended bias.

Section 9: Social media and the law

9.1 Any illegal or unlawful acts that can be committed using words or images can equally be committed using social media.

9.2 Posts on social media that violate the general principles listed in section 3 of this document could potentially be in breach of legislation such as:

- The Communications Act 2003
- The Contempt of Court Act 1981
- The Data Protection Act 2018
- The Defamation Act 2013
- The Malicious Communications Act 1988
- The Offences Against the Person Act 1861
- The Protection From Harassment Act 1997
- The Sexual Offences Act 2003

9.3 Other legislation relating to social media use include the following:

- Human Rights Act 1998
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

9.4 Article 8 of the European Convention on Human Rights (listed in Schedule 1 of the Human Rights Act 1998), covers the right to respect for private and family life. As such, when monitoring social media use by employees or students, members of staff should avoid doing anything that might constitute an invasion of their privacy.

Section 10: Disciplinary action over social media use
10.1 All employees are required to adhere to this policy. Any breaches may lead to disciplinary action. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the organisation, may constitute gross misconduct and lead to summary dismissal.