PLYMOUTH MARJON UNIVERSITY

Social Media Policy

Purpose

This policy outlines our expectations of the use of social media for staff, students, and others professionally associated with Plymouth Marjon University. Social media covers any online platform through which people publish, discuss, share, or otherwise communicate.

Principles

- The University recognises that social media brings tremendous opportunities, but also that it can do great harm, particularly to wellbeing and reputations. This policy recognises the responsibilities of staff and students to the University, but also the responsibility of the University to staff and students.
- The aim of this policy is to support students and staff to use social media in a safe and professional manner.
- This policy is written in line with our values, which encourage and celebrate individuality, but which also recognise our common humanity. The policy recognises that our ambitions for the University and for individual staff or students can be supported by social media or harmed by it.
- This policy covers use of social media by both staff and students in various situations including:
    - when clearly identifiable as associated with the University, for example in the profile or in the way a post is written
    - when interacting in a personal capacity and not specifically identifying with the University, and;
    - when running a corporate (University branded) social media account.
- This policy covers use of social media whether used in ‘working time’ or not.
- This policy does not impact on legitimate academic freedom of inquiry and aligns with our existing academic code of practice.

- While we use the term “staff and students” most frequently in this policy, the policy also covers those associated with Plymouth Marjon University in a professional context such as Governors or suppliers.
- There are several laws which staff and students should be aware of when using social media. These are listed in Appendix 1 and cover issues such as defamation, malicious falsehood, harassment, advertising standards and Prevent.

Other policies

- This policy should be read in conjunction with the Harassment and Dignity at Work policy, the Student Misconduct Procedures (Section 15 of the Student Regulations Framework), the Privacy Duty Policy, and the Photography and Filming Policy.

Contents

1. Context

Social media can be an important tool for colleagues’ professional activity and provide a helpful platform for profile raising and enhancing networks. It is recommended that colleagues using social media for both professional and personal reasons maintain separate accounts for these purposes as the audiences for each activity are often distinct.
Staff should ensure that if they do discuss their work on social media, they should make it clear on their profile statement or elsewhere that the views expressed are their own and do not necessarily reflect those of the University.

All employees should consider what they are posting on their individual accounts and whether they would wish their colleagues, or our students to see it.

The University does not routinely monitor individuals' accounts but will investigate where concerns are raised. These might relate to statutory issues such as Prevent, professional issues such as fitness to practice, or issues related to other policies such as bullying or harassment.

If a concern is raised regarding content posted on a staff member's social media account and the post is considered to be misconduct (as defined in the University's Disciplinary Procedure), the University has the right to request the removal of content. In addition, the matter may be addressed through the University's Disciplinary Procedure. Serious breaches including, but not limited to, harassment or bullying of colleagues and the misuse of confidential information may constitute gross misconduct and may lead to action including dismissal. The University's response to any misuse of social media will be reasonable and proportionate to the perceived offence, the nature of the postings made, and the impact or potential impact on the University, on students or on members of staff.

Social networking sites may be referred to when investigating possible misconduct/gross misconduct. The University may also check social media presence before offering contracts of employment.

2. Content of posts

2.1 Professionalism and confidentiality online

- This section covers staff, students, and others associated with the University in a professional capacity. This might include Governors or key suppliers on major projects – referred to below as "other professional partners".
- Staff, students or other professional partners must not represent themselves or the University in a misleading way.
- Staff, students or other professional partners must not promote anything online which is defamatory or likely to bring the University into disrepute. This does not prevent people from leaving fair and honest online reviews.

- When identifying themselves with the University in their profile (for example "Student at Plymouth Marjon University") staff, students or other professional partners must state that all views are their own.
- Students on professionally accredited programmes should ensure they are aware of the requirements of their specific Professional, Statutory or Regulatory bodies regarding social media. They should specifically note that any posts that bring their future profession into disrepute can be seen as an offence by the relevant governing body and Plymouth Marjon University will be required to investigate in line with fitness to practice principles. Such programmes include but are not limited to Sports Therapy, Rehabilitation in Sport and Exercise, Speech and Language Therapy, Osteopathic Medicine, any teaching programmes, Psychology, Nursing, Assistant Practitioner, Nursing Associate and Youth and Community Work.
    - Students on any placements must not share anything online which could bring the reputation of their placement providers into disrepute or which breach professionalism or confidentiality rules, for example rules around commercial, clinical or educational confidentiality.
    - Staff, students, or other professional partners should not discuss the University's internal workings or reveal plans or activities that have not been communicated to the public or reveal intellectual property. Efforts to be transparent should not mean publishing private, internal or confidential information.
    - The content of group chats or private chats, if known about, may be seen as harassment or discrimination and could be subject to misconduct procedures.

2.2 Other people's personal data

- Staff and students should be careful not to post images of people (that can be identified as such) without permission. At events, it must be made clear if photos or film will be taken so that people can request to be excluded. Permission forms will be obtained in some circumstances, usually smaller events, workshops and visits, or shoots set up solely for promotional purposes.

- Staff and students must not name individuals in a way which makes them identifiable, and which could bring them into disrepute, or share anything likely to cause harm to individuals. It should be noted that this does not necessarily mean using their name as their job description could make them identifiable.
- Staff or students must not share confidential information about an individual.
- Students on placements must follow confidentiality procedures and must not share information about their workplace, colleagues, customers or clients.
- Staff and students must not use someone else's images or written content without permission and/or without acknowledgement.

2.3 Complaints online

- Genuine complaints should be dealt with under the standard University procedures, for either staff or students. Publishing complaints (formal or informal) online could be viewed as defamatory activity if they reveal personal information or if they are subsequently not upheld.

2.4 Personal reputation

- Students and staff are reminded that social media leaves a permanent record and is often used by potential employers to review the background of job candidates.
- Staff and students are also reminded that liking and sharing posts are frequently seen as endorsing views.

3. Reasonable use

- Staff may make reasonable and appropriate use of social media for personal purposes during working time.

- We recognise that we encourage the use of using your social media networks to promote Marjon, but we do expect this to be done in a timely way with consideration for other priorities and in line with core job responsibilities.

4. Concerns raised in social media

No staff should actively monitor personal student or staff accounts. However, if anyone (staff or student) is made aware of concerning social media activity they should raise this as below:

- Activity which may raise concerns about welfare of staff to your line manager or to your HR manager.
- Activity which may raise concerns about welfare of students, including concerns under the Prevent guidelines, to sws@marjon.ac.uk, or to the Students' Union.
- Activity which may negatively impact the reputation of the University, which may need careful management, or which may cause harm or distress to someone else to marketing@marjon.ac.uk.
- To report concerning activity or gain confidential support or advice, staff and students can use an anonymous form on MyMarjon and Antler, or can email sws@marjon.ac.uk.

5. Corporate social media accounts

A corporate social media account is one which identifies as being related to Plymouth Marjon University.

Partners of the University running accounts which identify as Marjon should follow the same rules as corporate accounts.

Students running accounts which are for Marjon clubs or societies should also follow these rules.

Closed groups do not have to comply with all the same rules as other Corporate accounts, in terms of set-up, sharing access with the marketing team, and frequent postings, though it should be noted that there are many other University policies that do apply to these accounts, such as the Harassment and Dignity at Work policy and the Student Misconduct Procedures (Section 15 of the Student Regulations Framework). Content of group chats should at all times be respectful and values based.

Those running such accounts should:

- Ensure that they get agreement from the Marketing department before beginning an account. This is to ensure that the department can keep track of accounts and as teams change, the account can be kept up to date. It is also to check whether we already have an account which meets the needs of that audience.
- Agree the name of the account with the Marketing department. For sports teams, the name should be agreed with the Marjon Sport Federation.
- Set the account up from a Marjon email address, not from a personal account. If possible, this should be a group address such as sws@marjon.ac.uk so that responsibility for the account can be shared across a team.
- Ensure that account profile information clearly states the purpose of the account and the hours it is monitored.
- Ensure that the account is kept up to date, posted from frequently, and questions are responded to promptly within operating hours.
- Ensure the name of the Account Manager (one central person) and any other administrators is sent to the Marketing department. This is important so that training can be kept up to date with all those running accounts, and in case of emergency such as hacking.
- Ensure that access to the account is given to the Marketing department, again in case of hacking or a post attracting significant negative comments. This can be through making a colleague an administrator, or sharing log in details.
- If someone posts a complaint or negative feedback about Marjon within a group you manage, then you should move to take the conversation offline as politely as possible. Do not let it escalate online. Please consult with the Marketing team before posting a reply to any complaint made on social media.

- Social media security policies and technologies change frequently, and as such our advice will be updated. It is important to follow the latest ways of working and guidance as set out by the Marketing department. This information is available on the Antler Marketing page. Key changes will be communicated widely on Antler and direct to managers of social media accounts.

5.1 Content of posts from corporate accounts

All posts from corporate accounts are representing the University, and as such you should make sure all posts promote the University positively.

- Consider carefully, and discuss with the Marketing department, if necessary, your content plan, in particular any posts which may have a negative impact on the University.
- Ensure your posts align with the values of the University, are respectful to others, and in line with other key policies, including our Harassment and Dignity at Work policy.
- Do not use accounts to criticise or argue with colleagues, students, customers, partners, or competitors.
- Only share verified and accurate information, and do not commit to something which the University does not intend to deliver. If a mistake is made, the page must be updated with a clear correction. If in doubt about a post, check with a suitable colleague.
- Be wary of liking or sharing posts with potentially offensive content, including offensive language.

5.2 Security of corporate social media accounts

Social media accounts are at risk of hacking. These guidelines minimise this risk and subsequent reputational damage, and the significant resource implications which follow a breach in security.

- Where several members of staff require access to the same social media account, there must be one agreed Account Manager. They are responsible for giving access to colleagues as appropriate, choosing strong and secure passwords and sharing them securely.
- The Account Manager must keep a log of all those with access to the account. Access to the account should be revoked when a colleague active on it moves on from their role. If access is through shared passwords, they should be secure and a combination of letters, numbers and symbols, and should be changed annually.
- Where students or staff are temporarily granted access, a new password should be created when they no longer require access.
- Auto-population (automatically completing the username and password at log in) should not be selected for social media accounts. When logging on to an account on a mobile device, the device should be password protected.
- Whenever available, the account should have two-factor authentication enabled.

Document Details

Issue: 0.3

Created by: Katy Willis, PVC, Student Success

Review date: Feb 2024

Agreed on: April 2024 (ELT), 1st May 2024 (Senate)

Agreed by: ELT, Senate

Frequency of review: Every 2 years and as required.

Appendix 1: Relevant Laws to be Aware of

There are several pieces of legislation relevant to the use of social media and these are listed below. Staff and students using social media should be mindful of the following legal risks and acts.[1]

- Defamation: posting untrue content adversely affecting a person's or organisation's reputation, which has caused, or is likely to cause, harm
- Malicious falsehood: posting untrue and damaging content with an improper motive, resulting in financial loss for the subject
- Harassment: subjecting someone to a course of conduct that causes them distress or alarm, including stalking, trolling and cyber-bullying
- Intellectual property infringement: posting content which copies a substantial part of a work protected by copyright
- Breach of confidence: posting confidential information. Students and staff must familiarise themselves with the confidentiality rules of their area of the university. For example, healthcare or educational settings require the respect of confidentiality.
- Malicious Communications Act 1988: prevents conveying a threat, a grossly offensive or indecent message or false information with the intention to cause distress or anxiety to the reader or recipient.
- Section 127, Communications Act 2003: prevents the use of public electronic communications equipment to send a message that is false, grossly offensive, or of an indecent, obscene or menacing character, whether received by the intended recipient or not.
- Computer Misuse Act 1990: prevents the unauthorised access, modification and use of computer material or the use of a computer to assist in a criminal offence, including accessing confidential information and thereby impersonating another person through social media.

[1] Information reproduced from Thomson Reuters, Practical Law and University of Liverpool's Social Media Policy

- Prevent Duty Guidance (from Section 26(1) of the Counter-Terrorism and Security Act 2015): requires the University to have due regard to the need to prevent people from being drawn into terrorism.
- The Public Sector Equality Duty (Section 146 of the Equality Act 2010): requires the University to have due regard to the need to eliminate unlawful discrimination, including bullying, harassment and victimisation; to promote equality of opportunity between different groups; and to foster good relations between different groups.
- The Consumer Protection from Unfair Trading Regulations 2008, which protect consumers from unfair or misleading advertising practices, and require the university to ensure we give prospective students everything they need to make an informed decision about their education. This would also prohibit us from providing misleading information about, for example, prospects after graduation.

  Relevant legislation includes:

  - Communications Act 2003
  - Computer Misuse Act 1990
  - Consumer Protection from Unfair Trading Regulations 2008
  - Copyright, Designs and Patents Act 1988
  - Counter Terrorism and Security Act 2015 (Prevent)
  - Criminal Justice and Immigration Act 2008
  - Data Protection Act 1998
  - Data Retention Investigatory Powers Act 2014
  - Defamation Act 2013
  - Education (No. 2) Act 1986 (Freedom of Speech)
  - Education Act 1986; Education Reform Act 1988 (Academic Freedom)
  - Employment Rights Act 1996
  - Equality Act 2010
  - Freedom of Information Act 2000
  - Freedom of Information (Scotland) Act 2002
  - General Data Protection Regulation (GDPR) 2016
  - Human Rights Act 1998

- Malicious Communications Act 1988
- Obscene Publications Act 1959 and 1964
- Police and Criminal Evidence Act 1984
- Police and Justice Act 2006
- Prevention of Terrorism Act 2005
- Protection from Harassment Act 1997
- Protection of Children Act 1978
- Public Order Act 1986 (as amended by the Racial and Religious Hatred Act 2007)
- Regulation of Investigatory Powers Act 2000
- Terrorism Act 2006