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

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.

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

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 wit9eW*nBT/F3 12 Tf1-3(andal)3(person))-nnepfeBT1 0 595

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

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.

anager. They are responsible

Document Details

Issue: 0.3

Created by: Katy Willis, PVC, Student Success

Review date: Feb 2024

Agreed on: April 2024 (EF2u71 0 595.32 841.92 reW*nBT/F3 12 Tf1 0 0 1 72 595.24 Tm0 g0 EMC

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

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