UNIVERSITY OF LIVERPOOL

SOCIAL MEDIA COMPLIANCE POLICY

EXTERNAL RELATIONS, MARKETING AND COMMUNICATIONS DEPARTMENT

Document history

Author	Jo Carr
Role	Deputy Director of Communications and Public Affairs
Owner	External Relations, Marketing and Communications
Approved by	Environment, Systems and Sustainability Board
Approval date	March 2018
Review date	March 2019

Contents

1.1 Introduction 4
1.2 Policy objectives 4
1.3 Definitions 4
1.4 Legal risks 5

2. Staff 6
2.1 Overarching requirements 6
2.1.1 Policy acceptance 6
2.1.2 Appropriate use 6
2.1.3 Public Interest Disclosure (whistleblowing) 6
2.2 Staff contributing to corporate accounts 6
2.2.1 Setting up a new social media account 6
2.2.2 Social media account management 6
2.2.3 Social media posts 7
2.2.4 Accessibility 7
2.2.5 Account security 8
2.2.6 Escalating concerns and issues 8
2.2.7 Social media in an emergency 8
2.3 Individuals' personal and professional accounts 9
2.4 Other relevant policies and guidelines 9

3. Students 10
3.1 Social media posts 10
3.2 Account security 11
3.3 Further guidance 11

Appendix A – Legislation 12

1.1 Introduction

Social media channels provide important and exciting opportunities for the University and its constituent parts to communicate and engage with a wide range of audiences and stakeholders. These channels also provide a range of professional and personal opportunities for staff and students.

However, there are also a number of risks associated with the use of social media which could ultimately impact on the University's reputation.

This policy provides guidance to staff and students on how to safely and productively use social media to maximise the range of benefits it offers whilst mitigating associated risks. In particular, it provides information on: responsibilities when communicating via corporate social media accounts; expectations of staff on individual personal and professional accounts; and expectations of students in relation to social media.

Staff should comply with sections 1 and 2 of the policy. Students should comply with sections 1 and 3 of the policy.

1.2 Policy objectives

- To provide staff and students with information on University requirements and expectations regarding social media
- To ensure a consistent approach to social media across the institution
- To set out the legal risks associated with social media use
- To ensure staff and students do not compromise their personal security or the security of University information assets
- To set out the responsibilities of users of corporate social media accounts
- To support users of corporate social media accounts to mitigate the risks associated with social media, protecting themselves as well as the University
- To clarify the expectations of staff and students using social media in an individual professional or personal capacity
- To outline channels for escalation of issues or concerns
- To signpost staff and students to resources which will support them in enhancing their social media presence and that of the University.

1.3 Definitions

Social media are websites and applications that enable users to create and share content or to participate in social networking.

Examples of popular social media sites include, but are not limited to:

- LinkedIn
- Twitter
- Facebook
- YouTube
- Instagram
- Snapchat
- Flickr
- Yammer
- Yahoo/MSN messenger
- Wikis and blogs
- Weibo

- WeChat
- Whatsapp

A corporate social media account is any account run by a faculty, department, school, group or other function which sits within the University.

1.4 Legal risks

There are a number of pieces of legislation relevant to the use of social media and these are listed in Appendix A. Staff and students using social media should be mindful of the following legal risks and acts in particular.[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. The University's Information Asset Classification Policy details how information assets should be classified and treated – from public information to that which is confidential or secret. Students and staff must also familiarise themselves with the confidentiality rules of their area of the university. For example, healthcare and veterinary settings require the respect of confidentiality in clinical cases.
- 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.
- 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.

[1] Information reproduced from Thomson Reuters, Practical Law

2. Staff

2.1 Overarching requirements

2.1.1 Policy acceptance

This policy forms part of the University's contractual requirements of staff members.

2.1.2 Appropriate use

Staff may make reasonable and appropriate use of social media from University of Liverpool devices. Time spent on social media during working hours should not interfere with other duties.

2.1.3 Public Interest Disclosure (whistleblowing)

Any disclosure of serious malpractice, corruption, wrongdoing or impropriety should be made to either the Deputy Vice-Chancellor or the Director of Human Resources. Where an employee releases such information through social media, the University's Public Interest Disclosure Policy will be initiated before any further action is taken.

2.2 Staff contributing to corporate accounts

2.2.1 Setting up a new social media account

There are over 250 live corporate social media accounts for the University of Liverpool. Before creating a new corporate social media account it is therefore vital that staff consider whether there is a different audience or set of objectives which cannot be met through an existing account. Before opening a new account an activity plan should be created which considers: the target audience and their information needs; the content to be shared; how producing content and monitoring the account will be resourced; and how this account sits together with those already established across the University.

If a new account is to be established, its name should begin with 'livuni' for consistency with other University accounts. The new account and account manager must be registered centrally with External Relations, Marketing and Communications (ERMC) by emailing socialmedia@liverpool.ac.uk. ERMC maintains an asset register of all corporate social media accounts for the University with a designated account owner. This is important for emergency situations and to keep colleagues across the institution up to date with policy changes and training opportunities.

A more detailed list of considerations and guidance on setting up a new social media account can be found in the Social Media Toolkit.

2.2.2 Social media account management

All corporate social media accounts must adhere to the University's brand guidelines and the account profile information should clearly state the purpose of the account and the hours during which it is monitored.

It is important that all social media accounts are kept up to date, posted from regularly and monitored on a frequent basis. Questions should be responded to promptly within operating hours.

Where several members of staff require access to the same social media account, there must be an agreed overall account manager.

2.2.3 Social media posts

All posts from corporate social media accounts represent the University. It is vital that messages posted are carefully considered, appropriate and do not damage the reputation of the University or otherwise bring it into disrepute. Safeguards should be put in place to minimise the risk of communication errors via social media, including checking content with a colleague before publishing.

Posts must be in line with the values and ethics of the University of Liverpool and all relevant university policies, including Regulations for the Use of IT Services. Those posting content on corporate social media accounts **must not**:

- post or promote content which harasses, bullies or otherwise intimidates
- post or promote content which instructs, causes or coerces others to harass, bully or otherwise intimidate
- post or promote content intended to incite violence or hatred
- post or promote abusive content relating to an individual's age, disability, gender reassignment, marriage/civil partnership, pregnancy/maternity, race, religion or belief, sex or sexual orientation.

Content posted or promoted on corporate accounts must be respectful of others and courteous. Corporate accounts must not be used to criticise or argue with colleagues, students, customers, partners or competitors.

When posting on an account, it is vital to have legal considerations in mind (see section 1.4). This includes, but is not limited to, ensuring that posts do not breach confidentiality, make defamatory comments or breach copyright. Communications through social media **must not:**

- include confidential information about an individual or organisation
- discuss the University's internal workings or reveal future plans that have not been communicated to the public
- reveal intellectual property
- breach the professionalism and confidentiality rules of their area of the university. For example, Health Sciences, Dentistry, Medical and Veterinary accounts must not breach confidentiality in clinical cases
- use someone else's images or written content without permission and/or without acknowledgement.

It is also important that content is accurate and does not commit to something which the University does not intend to deliver. If a mistake is made, it is important to be transparent and update the page with a correction.

2.2.4 Accessibility

All film content which is externally produced or produced in advance for use in a social media campaign must have subtitles for accessibility purposes.

It is accepted that some film content for social media is either livestreamed or produced for immediate use (given the immediacy of the channel). In such instances, subtitles are not required but a full transcript of audio content of such clips should be made available on request.

2.2.5 Account security

Social media accounts are at risk of hacking and this can cause significant reputational damage and potentially serious misinformation for stakeholders. There are also considerable resource implications following on from any breach in security such as a compromised social media account.

Where several members of staff require access to the same social media account, there must be an agreed overall account manager. S/he is responsible for choosing strong and secure passwords which are different from MWS passwords and in line with password guidance provided by CSD. The account manager must also ensure passwords are shared and stored securely via a solution such as LastPass and not in files on shared drives or on paper. Further guidance for securely storing passwords is under creation and password sharing will remain under review. Where viable alternative solutions become available, the policy will be updated to reflect this.

The social media account manager is responsible for maintaining a full log of staff with access to the account's password and the password must be changed whenever one of those staff members moves on to a different role or different institution. In any case, the password must be changed on a quarterly basis and social media account managers will receive a reminder to do so from ERMC.

Where other colleagues or students are granted temporary access to a corporate social media account (e.g. as part of a social media takeover), a secure temporary new account password must be created and then changed back once the takeover is complete.

In cases of emergency, such as hacking, the press team may need urgent out of hours access to any corporate social media account. Each social media account manager must therefore ensure that the press team has suitable access to their shared passwords.

Auto-population must not be selected for access to any social media account on desktop devices. Where staff are accessing corporate accounts on mobile devices, it is vital to ensure a suitable screen lock is enabled on the mobile device to prevent unauthorised access. Staff should also secure accounts with 2-factor authentication.

2.2.6 Escalating concerns and issues

If a social media account has been hacked or a post from a corporate account attracts a number of negative comments and it is not clear how best to respond, staff should flag this with ERMC and seek guidance.

Staff should not actively monitor individual staff or student accounts. However, if a staff member notices, or is made aware of, social media activity on a staff or student account which raises welfare concerns or constitutes misconduct, they should alert ERMC by emailing socialmedia@liverpool.ac.uk or ringing 0151 795 7314.

2.2.7 Social media in an emergency

Social media provides important information channels for staff, students and wider stakeholders during an emergency situation and it is vital that the information provided is timely, consistent and accurate.

All communications on social media from the University in an emergency situation will be issued via the central university social media accounts (@livuni). In order to minimise the risk of issuing conflicting and/or incorrect information, it is vital that all other corporate social media accounts do not post information or updates during a live incident.

2.3 Individuals’ personal and professional accounts

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.

Individuals’ personal and professional accounts should not use University of Liverpool branding and, if staff 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. The University does not and will not monitor individuals’ accounts. However, 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.

2.4 Other relevant policies and guidelines

Regulations for the Use of IT Services
Information Asset Classification Policy
Disciplinary Procedure
Public Interest Disclosure (Whistleblowing) Policy
Dignity at Work and Study Policy
Policy on Student Conduct and Discipline

3. Students

Students' presence on social media is a public record which is interlinked with individual reputation. Social media can be a positive tool but it is important to carefully consider post content and account security in order to mitigate the associated risks.

Posting offensive, inappropriate or unlawful material can have a number of serious consequences, including, but not limited to:

- significantly impacting on an individual's academic and long-term employment prospects
- 'fitness to practise' processes for Health Sciences, Dentistry, Medical and Veterinary students
- damaging the University's reputation
- legal action
- the University taking disciplinary action.

Poor account security can result in account hacking and identity theft which also have serious legal, reputational, academic, employment and financial implications.

3.1 Social media posts

The University's policy framework, including the Policy on Student Conduct and Discipline and the Bullying and Harassment Policy, commits to ensuring that it provides a safe and welcoming environment in which all staff and students can flourish and achieve their potential.

The University expects its students to act in line with these commitments.

When posting on social media, students **are required to**:

- conduct themselves in a manner which demonstrates respect for university staff, fellow students and property, and for other members of the local community in general
- act in line with the University's Policy on Student Conduct and Discipline, which governs expectations of student conduct both online and offline
- act in line with the professionalism and confidentiality rules of their area of the university. For example, Health Sciences, Dentistry, Medical and Veterinary students must retain professionalism and respect confidentiality in clinical cases. Research students must also be aware of rules governing the recruitment of study volunteers
- ensure their posts do not raise any copyright or intellectual property issues or the other legal issues outlined in 1.4 above
- act in line with the University's Regulations for the Use of IT Services.

When posting on social media, students **must not**:

- breach others' privacy through sharing or promoting private information, images or other content
- fraudulently assume the identity of another
- post or promote content which harasses, bullies or otherwise intimidates
- post or promote content intended to incite violence or hatred
- post or promote abusive content relating to an individual's sex, sexual orientation, religion or belief, race, pregnancy/maternity, marriage/civil partnership, gender reassignment, disability or age

- post or promote content threatening to cause harm
- repeatedly make unwanted or unsolicited contact with another person
- post or promote content which damages, or has the potential to damage, the University's relationships with the local community or other bodies or organisations
- use the University logo or any other University images or icons on personal social media sites.

Failure to act in line with the above may result in the University taking disciplinary action. Students must familiarise themselves with the Policy on Student Conduct and Discipline. Of particular note for social media is Appendix I, which sets out a number of non-academic misconduct offences and indicative sanctions.

3.2 Account security

It is important that students protect their online identity against hacking by choosing strong and secure passwords, different from passwords they use for other accounts. CSD's password guidance offers advice on how best to construct strong passwords.

In addition, instances of students' accounts being hacked through use of their mobile devices are increasing. Students are responsible for ensuring that they do not permit or give opportunity to anyone else to use their account. If an inappropriate post is made by someone else using their account, they may be regarded as having responsibility for this if they have not adequately protected their account. It is therefore vital that students ensure a suitable screen lock is enabled on their mobile devices to prevent unauthorised access to their social media accounts.

It is also recommended that students do not enable auto-population of their usernames and passwords for social media accounts and that they set up two-factor authentication. Guidance on how to do this can be found in the Student Social Media Toolkit.

3.3 Further guidance

Further guidance and advice on how to use social media can be found in the Student Social Media Toolkit.

Appendix A - Legislation

Relevant legislation includes:

- Communications Act 2003
- Computer Misuse Act 1990
- 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
- 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