University of Buckingham

Social Media Policy

Document Control

Changes History

Version	Date	Author	Recipients	Purpose
1	May 2018	J O'Dowd & J Richards	All stakeholders	Digital

Related policy statements and documents[1]

- Use of University Computers and Data Networks
- Equality and Diversity Policy
- Dignity at Work and Study Policy and Procedures
- University of Buckingham Library Social Media Policy

Authorisation

Name	Date
Senate	

Distribution

University Intranet. Email notification to all stakeholders

[1] All related policy documents can be found within Section 5 (General Policies and Regulations) of the Regulations Handbook on the university intranet, with the exception of the Library Social Media Policy.

1. Introduction

The University of Buckingham recognises the importance and benefits of social media. However, there is the potential for significant risks associated with inappropriate use of social media.

The university aims to provide a safe, secure and supportive environment **for all staff and students** to engage with the wider community.

This policy intersects with the general principles of dignity at work and study; equality and diversity; and appropriate use of the university's computers and data networks, as outlined in the relevant sections of the Regulations Handbook referenced above. It relates specifically to use of official social media channels relating to university business, although social media usage outside of the university by members of staff or students should also include a consideration of reputational risk by association (see in particular section 9 below on Declarations).

2. Scope

2.1 Platforms

Social media describes dynamic and socially interactive, web-based applications that allow people to create and exchange content.

Example sites include, but are not limited to:

- Multimedia and social networking sites, such as Facebook, LinkedIn and YouTube
- Internal or external blogs and microblogs including Twitter
- Community discussion forums such as Yahoo! Groups and Google Groups
- Review or rating forums such as TripAdvisor, BBC Have your Say and MoneySavingExpert
- Wikis, such as Wikipedia
- Content communities – any site where you can post text, photos and videos such as YouTube, Pinterest, Instagram, Flickr, Google+ and Tumblr.

2.2 Who does this apply to

This policy applies to **all university staff and students** and to all social media communications that represent the university, whether those are officially-registered or informal.

3. Purpose

The aim of this policy is to help students of the university to use social media sites without compromising their personal security or the security of university information assets. The main concern of this document is about proper use of social media with regards to university regulations and reputational issues: best practice and advice on how to use social media to good effect for marketing and communications are dealt with elsewhere.

It is the responsibility of each member of staff and student to comply with this Policy. The standards expected of each member of staff or student do not change because they are communicating through social media rather than face-to-face or through traditional media.

Students in breach of the policy will be liable to university disciplinary actions. Inappropriate use of social media may constitute a criminal offence. In such cases the university may contact the Police.

Procedures will be put in place to ensure that effective implementation of the principles that underpin the Social Media Policy.

4. Freedom of Speech and Academic Freedom

4.1. Nothing in this policy is intended to have the effect of limiting either freedom of speech within the law or academic freedom.

5. Distribution

5.1. This policy is published within Section 5 of the Regulations Handbook

6. Exceptions

6.1. There are no exceptions to this policy.

7. Authorisation and Change

7.1. This policy has been approved by Senate, and is maintained by the Student Conduct Manager team.

7.2. Any questions relating to this policy should be referred to the Student Conduct Manager team. The Quality Assurance Office can advise about amendments to this policy; these should accord with procedures outlined in Published Information Policy, and the approval lines recorded in the University Policy Matrix.

8. Posting on Social Media

8.1. Staff and students are personally responsible for what they communicate on or through social media and they must adhere to the standards of behaviour set out in this policy and any related policies.

8.2. Staff and students should post content with the understanding that everything will be public and permanent, regardless of the privacy settings they assume are applied.

8.3. The university's name, identity and logo may only be used as authorised by the university.

8.4. Staff and students must not use social media for any of the following:

8.4.1. To post material that could be deemed to be threatening, harassing, discriminatory, illegal, obscene, defamatory, libellous, or hostile towards any individual or entity.

8.4.2. To express support for illegal activities or organisations.

8.4.3. To air internal grievances, infringe on the rights and privacy of colleagues or students or make ill-considered comments or judgments about staff or students.

8.4.4. To share confidential or sensitive information about the university and its associated entities, such as funding bids, personnel matters business strategy, or non-public news.

8.4.5. To infringe or violate someone else's rights.

8.4.6. To post personally identifiable information that could be used to locate any individual without that person's written permission.

8.5. No personal information, including photographs and videos, should be shared on social media without the consent of the individual to whom it relates. Staff and students should, therefore, never post other students' and/or staff and/or a third party's personal information without their consent.

8.6. It is the responsibility of all staff and students to check the terms and conditions of a social media account and/or website before uploading material to it. By posting material to social media accounts and/or websites, individuals may be releasing ownership rights and control of the content.

8.7. Staff and students should be aware that social media content may easily be shared with the public, including the university's students and the media, and inappropriate use could damage their own reputation and career prospects, as well as the reputation of the university.

9. Declarations

9.1. When not using an official university platform but using a personal social media account to discuss university business, staff and students should be aware of the risks of bringing the university into disrepute by association, and should include in their communications, where appropriate, a disclaimer stating that the views expressed are their own and not those of the university.

9.2. Staff and students should be open about any conflict of interest and declare any financial or commercial interests when posting material online using any platform.

10. Cyberbullying

10.1. The university will not accept any form of bullying or harassment by or of members of university staff or students.

10.2. The following examples illustrate, but are not limited to, the types of behaviour, displayed through social media communications, which the university considers to be forms of cyber-bullying:

- maliciously spreading rumours, lies or gossip
- intimidating or aggressive behaviour
- offensive or threatening comments or content
- posting comments/photos etc. deliberately mocking an individual with the intent to harass or humiliate them.

10.3. Cyber-bullying may also take place via other means of electronic communication such as email, text or instant messaging.

10.4. Any member of staff or student who is experiencing cyber-bullying by another student or a member of staff, will have the full support of the university. If a student feels they are being bullied, harassed or victimised, the university's Dignity at Work and Study policy outlines the procedure to be followed; or the matter should be referred to the Student Conduct Manager team in the first instance.

11. Monitoring Social Media

11.1. The university reserves the right, within the law, to monitor, intercept and review, without further notice, staff and student activities using its IT resources and communications systems, including but not limited to social media postings, to ensure that its rules are being complied with and such activities are for legitimate purposes.

11.2. The Freedom of Information Act 2000 may apply to posts and content that individuals have uploaded to official university websites, or any other website belonging to a public authority.

12. Incidents and Response

12.1. Any suspected breaches of this policy should be directed to the Student Conduct Manager team (in relation to students) or Human Resources (in relation to staff).

12.2. Where it appears that a breach of this Policy has taken place, relevant members of staff will investigate and review what has happened and decide on the most appropriate and proportionate course of action, in line with the policies referenced above.

12.3. Any breach of this policy may result in disciplinary action up to and including exclusion/termination of registration, or dismissal in the case of staff.

12.4. Any disciplinary action will be taken in accordance with the procedures outlined in related university rules and regulations.

12.5. Disciplinary action may be taken regardless of when the breach is committed and regardless of whether any university equipment or facilities are used in committing the breach.

12.6. Where conduct may be illegal criminal offence, the university may report the matter to the police. Beyond that, any member of staff, student or third party may pursue legal action against individuals, if they choose to do so.

12.7. The University has the right to request the removal of content from an official social media account and from a personal account if it is deemed that the account or its submissions pose a risk to the reputation of the university or to that of one of its members.

12.8. Staff or students who post views, opinions or images online in breach of University Guidelines may be subject to disciplinary action. Individuals' actions may also be subjected to prosecution under UK criminal and civil legislation

12.9. If members of staff are subject to offensive or unacceptable content via social media, it should be reported to Human Resources.

12.10. Any concerns in relation to fake accounts (whether relating to the university or an individual) should be reported to the Student Conduct Manager team.

13. Official Accounts, Ownership and Acknowledgement

13.1. All Official University social media accounts must be registered with the Marketing team, or the Library if the platforms relate to the library-specific Facebook and Twitter accounts. Staff/student(s) of the university who wish to create a social media page on behalf of a group of which they are affiliated (e.g. their department or research group), should seek the approval of the Director of Recruitment and Admissions before creating a social media account.

13.2. All university pages must have associated staff member who is identified as being the information asset owner and who is responsible for its official affiliation of the university. Individuals responsible for representing official social media accounts on behalf of the University of Buckingham when posting on a social media platform, clearly acknowledge this.

14. Security of University managed social media accounts

14.1. University members are responsible for ensuring that passwords and other access controls for official university social media accounts are of adequate strength and kept secure. Under no circumstances should passwords be shared except with other administrators authorised to use the relevant university account. Passwords must be changed when an account administrator leaves the university or changes role within the university. Staff should be familiar with privacy settings and ensure that these are appropriate for both content and intended audience.

14.2. Passwords must be changed when there is a compromise or suspected compromise of an official university social media account. Using two factor authentication to access official university accounts is good practice but is not required.

14.3. All university members must comply with the university's Information Security Policy (Use of University Computers and Data Networks) at all times.

15. Review of Policy

15.1. The policy will be reviewed annually.

15.2. The impact of this policy will be monitored regularly to reflect the changing online environment and technologies.