

Social Media Policy

1. Position Statement

The University recognises the numerous benefits and opportunities that a social media presence offers for all members of the University. The University is committed to freedom of expression and encourages its staff and students to exchange ideas and participate in discourse and debate. Our approach is therefore to support University members to engage with the wider community, while providing appropriate guidance on good practice to ensure such engagement is safe and responsible.

University members are expected to maintain their knowledge of relevant University policies and guidance which apply in this context. This Policy should be read alongside the University's [Social Media Guidance \(PDF, 399kB\)](#) document.

2. Authorisation and Review

This policy has been approved by the University Web Board on 9th April 2015 . Any questions relating to this policy should be addressed to the Public Relations Office. The impact of this policy will be monitored regularly to reflect the changing online environment and technologies. It will be reviewed annually by the Social Media Steering Group with any substantive amendments to be approved by the Web Board.

3. Scope of the Policy

Platforms

For the purposes of this policy, social media is defined as any online interactive communication tool which encourages participation and exchanges. Current examples include Twitter, Facebook, YouTube, Skype, Instagram, Pinterest, Yammer and LinkedIn but the policy also includes the use of external internet messageboards and chat rooms. Any social media platform hosted on the University's domain is within scope of this policy.

Who it applies to

This policy applies to all University members (both staff and students) and to all social media communications that represent the University.

4. Conduct and interaction with other policies and regulations

Professional responsibilities apply regardless of the medium being used. All social media communications that represent the University must comply with relevant University policies that address staff and student conduct:

- [Acceptable Behaviour Policy \(staff\)](#) (PDF, 343kB)
 - [Rules of Conduct for Members of Staff](#)
 - [Student Agreement](#)
 - [Student Disciplinary Regulations](#)
 - [Information Security Policy](#)
-

5. Security of University managed social media accounts

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.

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.

All University members must comply with the University's [Information Security Policy](#) at all times.

6. Incidents and Response

Any suspected breaches of this policy should be directed to the Secretary's Office (in relation to students) or Human Resources (in relation to staff).

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 in section 4.

If members of staff are subject to offensive or unacceptable content via social media, it should be reported to your line manager. The annex of the University's [Acceptable Behaviour Policy](#) (PDF, 343kB) details sources of support that are available to staff in such situations. The University also has a Policy and Procedure for Students on [Reporting Allegations of Bullying and Harassment](#), which includes sources of support and advice for students.

Any concerns in relation to fake accounts (whether relating to the University or an individual) should be reported to the Secretary's Office.

7. Insurance

The University holds libel and slander insurance to cover damages and legal costs that the University becomes legally liable to pay. These include:

- a) libels appearing in any publications normal to the University's business made by any employee;
- b) slanders made in the course of official University duties.

Libel in connection with any statement or view expressed on social media is only likely to be covered by the University's insurance if the social medium concerned is normal to the University's business. In certain circumstances, the insurance policy also provides an indemnity to individual employees.

8. Feedback and Further Information

The University welcomes all constructive feedback on this and any other policy. If you would like further information on social media, or wish to send us your comments on our Social Media Policy, then please contact: web-editor@bristol.ac.uk.

University guidance:

- University's [social media homepage](#)
- Information on [maintaining social media channels](#)
- University's [Twitter guidelines](#)
- [Mobile application guidelines \(PDF, 148kB\)](#)
- Relevant [IT Services courses](#)

Externally produced guidance:

- EDINA [Social Media Guidelines](#) (PDF, 327kB)
 - LSE [Guidance on Twitter](#) for academics and research (PDF, 1,270kB)
 - Vitae Innovative [Handbook of Social Media](#) for Researchers and Supervisors (Open University)
-