

Social Media Policy

Originator name:	Mike Hounsell
Department:	Marketing & Communications
Implementation date:	1 November 2014
Date of next review:	1 March 2015
Related policies:	Code of Practice on Freedom of Speech Data Protection Policy Dignity at Work and Study Policy Disciplinary Policy IT Services Acceptable Use Policy University Policy for Email Use by Staff

Version History

Version	Author	Revisions Made	Date
1	Karen Porter/Emma Chandler	First Draft	March 2014
2	Karen Porter/Emma Chandler	Second Draft	March 2014
3	Karen Porter	Third Draft	3 April 2014
4	Lynda Bewley	Fourth draft incorporating stakeholder feedback: IT, Centre for Wellbeing, Health and Safety, Legal, DVC Academic Affairs, Department of Sociology.	10 September 2014
5	Lynda Bewley	Final input from Legal and HR	26 September 2014
6	Lynda Bewley	Final EB Amends: 2.1.1.1 changed to allow for 'argument' relating to Academic Freedom; Clarification relating internet monitoring; job title corrections.	15 October 2014

Approval History

Equality Analysis

Version	Reviewed by	Comments	Date
1	Angie Cousins, Head of Equality and Diversity		

Committee Sign Off

Version	Committee Name	Date of Sign Off
5	Social Media Working Group	26 September 2014
6	Executive Board Committee	15 October 2015

1	Introduction
	<p>Effective use of social media can bring significant and measurable benefits to the University. These include opportunities to promote the institution’s success stories, develop national and international reach, improve student engagement and attract high quality staff and students.</p> <p>Social media channels can spread the University’s messages across the globe quickly and to a range of audiences at little or no cost and, unlike other traditional media channels, they provide instant feedback from our audiences.</p> <p>Along with these benefits come the risks inherent in managing something that is dynamic and unlimited in scale. These include the risk of reputational damage arising from misuse by staff, students or third parties, threats to the security of sensitive or confidential information, exposure to malware and a negative impact on productivity.</p>
1.1	Purpose
	<p>This Social Media Policy aims to mitigate the risks associated with employees’ use of social media. It provides all University of Surrey staff with a clear articulation of the institution’s expectations around the use of social media. The accompanying Social Media Toolkit encourages University of Surrey staff to use social media and gives guidance on how best to make the most of the key channels.</p>
1.2	Scope
	<p>This policy has been produced for all University of Surrey employees. A policy for University of Surrey students will be provided separately.</p>
1.3	Equality Analysis
	<p>There is potential for social media channels to be used for bullying and harassment of individuals. It is therefore important that the policy is considered alongside the Dignity at Work and Study Policy. Staff Development will include reference to this policy in induction and management training.</p>
1.4	Definitions
	<p>According to the Chartered Institute of Public Relations (CIPR), social media are: “Internet and mobile-based channels and tools that allow users to interact with each other and share opinions and content. It involves the building of communities or networks and encouraging participation and engagement.” This is the recognised definition for the purpose of this document.</p> <p>This policy refers to three different types of social media account:</p> <ul style="list-style-type: none"> • Professional University of Surrey Account – used by representatives of the University to communicate messages from a departmental, faculty or corporate perspective; managed by a Professional Account Administrator (see 2.1.1.4). • Professional Personal Account – used by an individual member of staff, who is identifiable as an employee of the University of Surrey through the content of their posts or their profile’s biographical information. • Private Personal Account – used by an individual primarily for non-work activity. <p>Social networks covered by this policy include, but are not limited to, Facebook, Twitter, LinkedIn, YouTube, Instagram, Pinterest, Google+ and Tumblr.</p>
1.5	Legislative context
	<ul style="list-style-type: none"> • Data Protection Act 1998 and accompanying guidance in the Information Commissioner’s Employment Practices Data Protection Code. • Human Rights Act 1998. • Regulation of Investigatory Powers Act 2000. • Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699). • Copyright, Designs and Patents Act 1988

1.6	Health & Safety Implications
	There is potential for social media channels to be used to cause emotional harm or mental distress to others. By producing this policy and its accompanying toolkit, the University hopes to minimise any distress to its staff caused by the misuse of social media.
2	Policy
2.1	Principles
2.1.1	Professional use of social media
2.1.1.1	<p>University of Surrey employees using social media in a professional capacity, either through a Professional University of Surrey account or a Professional Personal Account, should make sure that their communications do not do any of the following.</p> <ul style="list-style-type: none"> • Bring the University into disrepute. For example, by making defamatory comments about individuals, other organisations or groups, or the University; or posting images that are inappropriate, links to inappropriate content or using inappropriate language. • Breach confidentiality. For example, revealing confidential information owned by the University relating to its activities, finances, people, or business plans, or the personal data of any individual who has not given informed consent (in writing) for their data to be published. • Breach copyright. For example, using someone else's image or written content without their permission; failing to give acknowledgement where permission to reproduce something has been obtained • Do anything that may be considered discriminatory against, or bullying and harassment of, any individual. For example, making offensive or derogatory comments relating to sex, gender, race, disability, sexual orientation, religion, belief or age; using social media to bully another individual; or posting images that are discriminatory or offensive or linking to such content. • Breach the terms of service of the social network. Each social network has different terms of use and community guidelines, which must be followed. <p>The University does, however, recognise Academic Freedom whereby staff shall have freedom within the law to question and test received wisdom and to put forward new ideas and controversial or unpopular opinions, without placing themselves in jeopardy of losing their jobs or privileges.</p>
2.1.1.2	<p>Employees using social media in a professional capacity should use the same safeguards that they would with any other form of communication about the University in the public sphere. These safeguards may include (but are not limited to):</p> <ul style="list-style-type: none"> • ensuring that the communication has a purpose and benefit to the University • obtaining a manager's permission before starting a public social media campaign • getting an appropriate person to check the content before it is published • seeking advice if you are unsure of your objectives or required outcomes.
2.1.1.3	<p>There should be a clear reason or reasons to set up a Professional University of Surrey Account and processes put in place to ensure that it is monitored and updated regularly. For detailed guidance please refer to the Social Media Toolkit (which is available on Asset Bank: http://assetbank.surrey.ac.uk).</p>
2.1.1.4	<p>Where a Professional University of Surrey account has two or more users, one user should be assigned the Professional Account Administrator role. This person will be responsible for:</p> <ul style="list-style-type: none"> • ensuring that the account meets brand guidelines as specified in the Social Media Toolkit • making sure that the login details are shared only with those who have a real need to use the account • revoking access to the account where necessary, such as if an employee leaves the organisation • ensuring that all content produced for the account is in line with this policy • ensuring that the account is used regularly • reporting any incidents where the administrator feels that an employee has misused the social media account.

2.1.1.5	<p>Employees managing a Professional University of Surrey account are expected to remove any comments that fit into the categories outlined in 2.1.1.1. Additionally, users should also remove comments that are:</p> <ul style="list-style-type: none"> • spam, or trying to sell things • fraudulent, deceptive or misleading • in violation of any law or regulation. <p>Employees are encouraged to think carefully before removing users' comments, to ensure that users with good intentions do not feel that we are placing an unjustified restriction on their freedom of speech.</p>
2.1.1.6	<p>Social media users are encouraged to regularly check their accounts for messages and respond to any enquiries that they receive in a timely fashion.</p>
2.1.1.7	<p>Social media users who receive enquiries/approaches from media sources (newspapers, radio, TV) relating to their work at the University are encouraged to notify the University's PR & Communications Team for guidance about how to respond (as they would if they received approaches from the media via any other channel).</p>
2.1.1.8	<p>All employees using social media in their professional role at the University of Surrey are encouraged to read the University's Social Media Toolkit – available on Asset Bank (http://assetbank.surrey.ac.uk)</p>
2.1.2	<p>Personal use of social media</p>
2.1.2.1	<p>The University recognises that many employees will make use of social media in a personal capacity. University of Surrey employees using social media in a personal capacity should make sure that their communications do not do any of the following:</p> <ul style="list-style-type: none"> • Bring the University into disrepute. • Breach confidentiality. • Breach copyright. • Breach the terms of service of the social network • Do anything that may be considered discriminatory against, or bullying and/or harassment of, any individual. <p>Misuse as outlined above may be regarded as a disciplinary offence (See 2.1.1).</p>
2.1.2.2	<p>Employees who openly disclose that they work for the University of Surrey should include on their profile a statement or disclaimer explaining that the views expressed are theirs alone and that they do not necessarily reflect the views of the University. However, if the content of a post is inappropriate, a disclaimer would not prevent disciplinary action.</p>
2.1.2.3	<p>To avoid confusion, the University prohibits the use of its logo(s) on social media when used for non-business reasons.</p>
2.1.2.4	<p>Employees are encouraged to familiarise themselves with privacy settings for each social media platform and choose a privacy level that they consider to be appropriate. For more information about privacy settings, please refer to the University's Social Media Toolkit – available on Asset Bank (http://assetbank.surrey.ac.uk)</p>
2.1.2.5	<p>Employees are permitted to make reasonable and appropriate use of personal social media from the University's computers or mobile devices, provided that this usage is limited to official rest breaks. For more information, please refer to 2.2.2 below.</p>
2.2	<p>Procedures</p>
2.2.1	<p>Where it is found that an employee has misused social media, it may be regarded as a disciplinary offence in accordance with the University Disciplinary Policy. Examples of misuse are outlined in 2.1.1.1 and 2.1.2.1</p>
2.2.2	<p>The University reserves the right to monitor employees' internet usage in line with the IT Services Acceptable Use Policy and the University Policy for Email Use by Staff. In line with this, it may instigate an investigation into an employee's internet usage where there are suspicions that the employee has been using social media excessively for personal use when they should be working, or in a way that is in breach of the rules set out in these policies. Authorisation to instigate an investigation into an employee's internet use can only be done by either the Vice-President Human Resources or the Chief Information Officer, following consideration of a valid case for this from the individual's line manager.</p>

2.2.3	The University monitors mentions of its brand name and associated terms in order to identify any risks to reputation and to gather customer feedback. Only content that is available in the public domain is subject to monitoring. Data monitored is processed anonymously for analysis purposes and is not held by the University. University employees are advised to read the privacy guidance provided in 2.1.2.4.
3	Governance & Directory Requirements
3.1	Responsibility
	<p>This policy is owned by the University's Social Media Working Group. This is currently chaired by the Vice-President Marketing & Communications. It will be the responsibility of the group's Chair to ensure that the policy is implemented, communicated and reviewed on an annual basis.</p> <p>The group will regularly review the impact of the policy and the accompanying toolkit and ensure that any subsequent issues relating to the use of social media are dealt with through the most appropriate channels.</p> <p>Specific responsibilities for social media across the University are as follows.</p> <ul style="list-style-type: none"> • Reputational risk created by social media – Head of PR & Communications • Response to customer enquiries – Head of Market Insight & Data • Marketing opportunities – Head of Digital Marketing • Social media development – Social Media Co-ordinator • Internet usage monitoring infrastructure – Chief Information Officer • Disciplinary proceedings relating to social media – Vice-President Human Resources
3.2	Implementation / Communication Plan
	<p>Once approved, this policy will be posted, along with the Social Media Toolkit, on to the University's website and communicated via internal communications channels including:</p> <ul style="list-style-type: none"> • Leaders' Alert, SurreyNet, SurreyLife and NetNews. • HR will be asked to include the policy in their briefing to new staff during the induction process. • Updates to this Policy and ongoing guidance relating to best practice in social media will be posted to the Social Media blog: blogs.surrey.ac.uk/socialmedia
3.3	Exceptions to this Policy
	<p>In all cases where it is believed that this policy has been breached, considerable judgement will be exercised to consider the context behind the issue and the impact of the action.</p> <p>However, where it is found that an employee has misused social media, it may be regarded as a disciplinary offence in accordance with the University Disciplinary Policy.</p>
3.4	Supporting documentation
	<p>This policy should be read in conjunction with:</p> <ul style="list-style-type: none"> • the University's Social Media Toolkit • IT Services Acceptable Use Policy • University Policy for Email Use by Staff • Code of Practice on Freedom of Speech • Data Protection Policy • Dignity at Work and Study Policy • Disciplinary Policy