University of Liverpool

Social Media Compliance Policy

Reference Number	CSD-008
Title	Social Media Compliance Policy
Version Number	v1.2
Document Status	Under Review
Document Classification	Open
Effective Date	22 May 2014
Review Date	17 November 2017
Document Author/Owner	Computing Services Department (David Hill)
Approved by	Corporate Services & Facilities Committee (May 2012)
Implemented by	Information Security Officer
Monitoring of compliance	Faculty Information Security Managers/Corporate Communications
Comments	• **22/05/2014 - Annual Review/Update v1.0 – v1.1** • **31/07/2015 – Annual Review/Update v1.1 –v 1.2** • **18/11/2016 – Annual Review/Update (Student Guidance Link updated)** • **28/03/2017 – Under Review**

Social Media Compliance Policy

Table of Contents

1. Introduction

Information is a vital asset to any organisation, and this is especially so in the University which is a knowledge-driven organisation. Virtually all of our activities create information assets in one form or another. The Social Media Compliance Policy and its associated policies are concerned with managing the information assets owned by the University and used by Staff/Student(s) of the University in their official capacities.

2. Principles

The Social Media Compliance Policy helps staff/student(s) of the University to use social media sites without compromising their personal security or the security of University information assets.

The University has adopted the following principles, which underpin this policy:

- All information assets must be appropriately handled and managed in accordance with their classification.
- University information assets should be made available to all who have a legitimate need for them.
- The integrity of information must be maintained; information must also be accurate, complete, timely and consistent with other related information and events.
- All staff/student(s) of the University, who have access to information assets, have a responsibility to handle them appropriately and in accordance with their classification.
- Information asset owners are responsible for ensuring that the University classification scheme (which is described in the Information Security Policy) is used appropriately.

3. Objectives of this Policy

- To provide a definition of social media and to articulate the potential risks it poses to the University and its staff/student(s).
- To define the responsibilities of individuals for the use of social media for University purposes.
- To highlight the potential risks of using social media for personal use.
- To co-ordinate and oversee the response to violations in accordance with the requirements of UK legislation, regulation and University policies.
- To minimise the potential negative impact to the University, its customers and third parties as a result of incidents and violations.

4. Action Implementation

Procedures will be put in place to ensure that social media is used effectively and securely. The following principles apply:

- Staff/student(s) of the University who use social media for University purposes must ensure that ownership of the site is explicit and a record of the ownership is held by Corporate Communications.
- Defamation of character of University Staff/student(s) will not be tolerated (either through an official account or personal use).
- Staff/student(s) of the University must be aware of best practice guidelines before using social media.
- Staff/student(s) of the University must be aware of guidelines on security and privacy settings for the use of social media.

- Potential negative impacts to the University, customers and third parties as a result of incidents/violations through social media must be minimised.

5. Social Media

Social media are powerful communication tools but they carry significant risks to the reputation of the University and its staff/student(s). A prominent risk arises from the blurring of the lines between personal voice and institutional voice. For the purposes of this policy, social media is defined as *media designed to be disseminated through social interaction, created using highly accessible and scalable publishing techniques using the internet*.

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

- LinkedIn
- Twitter
- Facebook
- YouTube
- MySpace
- Flickr
- Yammer
- Yahoo/MSN messenger
- Wiki's/Blogs

All staff/student(s) of the University using social media tools, including via personal accounts, must be aware that the same laws, professional expectations, and guidelines apply at all times.

Any social media announcements not issued by the Corporate Communications team, which may include (but are not limited to) content, comments and opinions must not give the impression they are in anyway the explicit positioning of the University of Liverpool. Any official University position and comment must be approved by the University Corporate Communications Director or his or her representative.

6. Social Media Threats and Risks

Below is a table of examples of threats and risks associated with the use of social media:

Threats	Risks
Introduction of viruses and malware to the University network	• Data leakage/theft • System downtime • Resources required to clean systems
Exposure of the University and its staff/student(s) through a fraudulent or hijacked presence e.g. unofficial social media accounts	• Customer backlash/adverse legal actions • Exposure of University information assets • Reputational damage • Targeted phishing attacks on customers or employees
Unclear or undefined ownership of content rights of information posted to social media sites (copyright infringement)	• Customer backlash/adverse legal actions • Exposure of customer information • Reputational damage

	• Targeted phishing attacks on customers or employees
Use of personal accounts to communicate University owned information assets	• Privacy violations • Reputational damage
Excessive use of social media within the University	• Network utilisation issues • Productivity loss • Increased risk of exposure to viruses and malware due to longer duration of sessions

7. Social Media Use (Including Personal Use)

Information Asset Classification

The University's Information Security Policy defines the categories which are assigned to University information assets. Those assets which are classified as ***Confidential, Strictly Confidential*** or ***Secret*** must not be posted on social media sites. Postings must not contain personal information concerning students, employees, or alumni.

In addition staff/student(s) of the University should be aware of the social media terms and conditions and ownership of content **before** submitting. Staff/student(s) should familiarise themselves with key University policies including:

- University IT Regulations
- Information Asset Classification Policy
- Copyright Policy
- Data Protection Policy
- Intellectual Property
- Acceptable Use of Electronic Resources

Official Accounts, Ownership and Acknowledgement

All Official University social media accounts must be registered with Corporate Communications. 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 contact Corporate Communications before creating a social media account.

Please refer to Corporate Communications Social Media Officer to request and/or register a University social media account.

Reputation and Institutional Voice

Communication via social media sites and tools must protect the University's institutional voice by remaining professional in tone and in good taste. Staff/student(s) of the University who use personal social media accounts must not give the impression that their social media site represents the explicit positioning of the University of Liverpool. This should be considered when:

- Naming pages or accounts
- Selecting a profile picture or icon
- Selecting content to post

Names, profile images, and posts should all be clearly linked to the particular Faculty, School, Institute and Professional Service Department.

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. If you are responsible for representing official social media accounts on behalf of the University of Liverpool when posting on a social media platform, clearly acknowledge this.

University Logo

Use of the University logo should be in line with University policy. The University logo or any other University images or icons must not be used for personal social media sites. For more information on use of the University logo refer to http://www.liv.ac.uk/intranet/identity.

Content Publishing

Staff/student(s) of the University who are responsible for an official University social media account should ensure the target audience is aware of the purpose of the site and the limits of acceptable use.

Consideration

Anyone posting to a social media site should consider their message, audience, and goals, as well as a strategy for keeping information up-to-date.

University Affiliation

Wherever possible, posts to official University social media sites should be brief and redirect the audience to content that resides within the University website. When linking to a news article link to an official release on the University website instead of an external resource or site.

8. Content Removal

Staff/student(s) of the University must be aware that 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 staff/student(s).

9. Social Media Guidelines and Best Practice

For more information on the guidelines and expectations of use of social media as a staff/student of the University, please refer to:

- Social Media Guidelines
- Social Media Guide (Student specific)

10. Social Media Privacy and Security

For more information about online safety and how staff/student(s) can protect themselves when using social media please refer to the Computing Services website: http://www.liv.ac.uk/csd/security/online-security

11. Reporting Security Incidents

Any misuse or any use that may bring the University or one of its staff/student(s) into disrepute must be reported to the CSD Service desk. For more information please refer to the Information Security Incident Response Policy.

CSD Service Desk Contact Details

For all other CSD services and queries please refer to the CSD Helpdesk in the first instance. You can do this by:

- Logging an online support request: http://servicedesk.liverpool.ac.uk/
- Email: servicedesk@liverpool.ac.uk
- Telephone: 44567 (internal)
- Telephone: +44 (0) 151 794 4567 (external)

12. Legal Obligations and University Policies

This policy is aimed at all members of the University who have a responsibility for the use, management and ownership of University assets. This policy is part of the University Information Security Management System (ISMS) and should be read in conjunction with the Information Security Policy and its sub policies and relevant UK legislation. Further relevant policies and legislation are listed in Appendix A.

13. Compliance and Monitoring

All members of the University are directly responsible and liable for the information they handle. Members of staff are bound to abide by the University IT regulations by the terms of their employment. Students are bound to abide by the University IT Regulations when registering as a student member of the University.

Authorised members of the University may monitor the use and management of information assets to ensure effective use and to detect unauthorised use of information assets.

Appendix A – University ISMS Reference

- Regulations for the Use of IT Facilities at the University of Liverpool
- JANET Acceptable Use policy
- Information Security Policy
- Workspace and IT Equipment Security Policy
- Information Security Incident Response Policy
- Information Asset Classification Policy
- Information Security Review Policy
- IT Procurement and Third Party Security Policy
- Security Investigation Policy
- IT Asset Disposal Policy
- Procurement Policy
- Data Protection Policy
- Freedom of Information Policy
- Copyright Policy
- Card Payment Policy
- Records Management Policy
- Records Retention Policy
- Risk Management Policy
- Student/HR Disciplinary Procedures

Relevant legislation includes:

- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act 1988
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Data Retention Investigatory Powers Act 2014
- Counter Terrorism and Security Act 2015 (Prevent)
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Police and Justice Act 2006
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002

Relevant Regulation includes:

- PCI-DSS (Payment Card Industry Data Security Standards)