HERIOT WATT UNIVERSITY

Social Media Policy for employees and contractors

August 2016

POLICY

Approving authority:	University Executive
Consultation via:	Secretary's Board
Approval date:	22 August 2016
Effective date:	22 August 2016
Review period:	Two years from date of approval
Responsible Executive:	Secretary of the University
Responsible Office:	Governance and Legal Services, Marketing and Communications

HERIOT-WATT UNIVERSITY

SOCIAL MEDIA POLICY FOR EMPLOYEES AND CONTRACTORS

CONTENTS

POLICY

1. INTRODUCTION

This policy applies to professional and personal use of social media by employees, contractors and other people who undertake paid or voluntary work on behalf of the University.

The University is committed to make the most effective use of communications technologies to support learning, teaching, research recruitment and public relations and engage with our communities. In particular, external social media platforms - web based tools that allow instant interaction between users - greatly enhance our ability to communicate and network with colleagues, students and the public.

At the same time, it is essential to recognise and manage the legal, ethical and reputational risks arising from the use of social media communications platforms. Information, once published online, may remain in the public domain indefinitely. The University also recognises that many people use social media to communicate for work related, study and personal purposes and that the boundaries between professional and private use are increasingly blurred. Therefore, the University has a responsibility to set out its expectations for employees about acceptable and unacceptable use of social media, in line with its wider rules governing professional conduct.

This policy sets out a framework to promote effective use of social media for work, to maintain a safe, professional environment and protect the interests of the University and all members of the University community. Any breach of this policy could lead to disciplinary action up to and including dismissal and/or legal action.

2. PURPOSE

This policy and its supporting guidance aim to:

- Support appropriate use of social media for University academic and professional purposes;
- Clarify the boundaries between work-related and private use of social media;
- Safeguard the interests and privacy of our students, staff and stakeholders and retain their trust;
- Promote e-safety and privacy online;
- Maintain the security of our IT systems and infrastructure;
- Protect our intellectual property rights, information assets, financial interests and competitive edge;
- Maintain our reputation;
- Confirm what is acceptable and what is unacceptable behaviour in terms of social media usage;
- Comply with the law and help defend the University and its employees against legal action.

3. OBJECTIVES

3.1 Using social media in academic and professional life

Heriot-Watt University actively supports appropriate use of social media in academic and professional life. All colleagues using social media for University work purposes need to be aware that, while contributing to the University's social media activities, they are representing the University. Colleagues need to ensure that their use of social media is compliant with the law and the issues covered by this policy.

3.2 Identification of University social media accounts

All University social media accounts must be clearly identified as such, using the University branding and logo in the manner set out in the University Style Guide, which is available from Marketing and Communications.

3.3 Security of University social media accounts

Colleagues who manage University social media accounts are responsible for ensuring that passwords and other access controls are of adequate strength and kept secure. All official University accounts should be set up to be managed jointly by nominated staff using an account with shared login credentials specific to the account, using a strong password, so that authorised colleagues can add content in the absence of the main content provider. Under no circumstances should passwords for individual staff accounts be shared with others. Accounts should not be left open and unattended for any period. Anyone using a personal device to manage University social media accounts is responsible for ensuring that its operating system and anti-virus software are up to date and that the device is encrypted, and doubly protected by a strong password/encryption key in case of loss.

3.4 Intellectual property rights in University social media accounts

The content of University social media accounts created by colleagues on University business and associated intellectual property rights belong to the University. Where colleagues set up University social media accounts such as LinkedIn to build networks of contacts on behalf of the University, the relevant contacts need to be handed over to the University when the individual staff member leaves, as part of the leaver management process.

3.5 Use of social media in employee recruitment

The University is committed to fair, open and accountable employee recruitment and selection procedures. The University reserves the right to review public social media profiles as part of the recruitment process. However, any such searches must comply with Equality, Human Rights and Data Protection laws.

Hiring Managers may use social media to promote advertised posts to potential applicants and to identify potential candidates. However, in doing so, particular care must be taken to avoid unconscious bias. The University will also use other channels to publicise vacancies to avoid excluding potential applicants who do not use social media. Hiring Managers who wish to use social media such as LinkedIn to advertise a vacancy need to ensure the link to the vacancy on iRecruit is included and that their message is consistent with the criteria set out in the iRecruit posting.

Where the post advertised requires the successful candidate to demonstrate evidence of effective public engagement using social media, or an established research profile, evidenced by online publications and citations, the hiring manager must ensure that the job advertisement asks applicants to cite examples and links e.g. Google Scholar profiles or h-indexes and informs potential candidates that these will be reviewed as part of the selection process.

If the hiring manager reviews social media profiles as part of the recruitment process they must:

- ensure they have fully documented a specific and justified purpose for doing so
- not use the review to exclude applicants from interview; unless evidence of online public engagement or research publications is an essential criterion for the role
- review the social media profile after the short-listing process unless evidence of online public engagement or research publications is an essential criterion for the role

If a search of an applicant's public social media profile reveals information about the individual that presents serious legal or reputational concerns for the University, the hiring manager must seek advice from the HR Recruitment Consultant or another member of the Human Resources team.

3.6 Use of private social media accounts in public life

Where colleagues use a private account that identifies their relationship with the University they need to make clear that they are not communicating on behalf of the University. It is best practice to include an appropriate disclaimer, such as:

"The views expressed here are my own and in no way reflect the views of the University"

Where colleagues do not include such a statement on their private social media account(s), and are later found to be in breach of this policy and its guidelines on usage, appropriate disciplinary action may be taken.

3.7 Acceptable conduct online

In the online environment, as in all other aspects of University life, all members of the University community need to treat others with dignity and respect, as they themselves should expect to be treated, at all times, in accordance with our University values.

The University recognises that employees may use social media to express personal views. The University does not routinely monitor the content posted by employees or students using social media. However, the University has a responsibility to investigate and to take appropriate action to deal with all instances of misconduct involving employees and students that are drawn to its attention, whether they take place online or face to face.

Examples of personal conduct in a personal or professional capacity which may incur disciplinary action (up to and including dismissal for Gross Misconduct) and may also be breaking criminal or civil law include:

- Behaviour that could be considered discriminatory against, or bullying or harassment of, any individual, for example by: making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age; posting images that are discriminatory or offensive or links to such content;

- Breach of confidentiality, for example by: revealing confidential intellectual property or information owned by the University or another other organisation (such as a partner institution); or discussing the University's internal workings (such as agreements that it is reaching with partner institutions/customers or its future business plans that have not been communicated to the public);

- Breaching the privacy of students, colleagues or other people whose personal data is held by the University, though sharing of their personal data in contravention of the Data Protection Principles;

- Conduct which brings the University into disrepute, for example by: criticising or arguing with students, customers, colleagues, partners or competitors; making abusive or defamatory comments about individuals or other organisations or groups; or posting images that are inappropriate or links to inappropriate content;

- Breaching copyright, for example by: using someone else's images or written content without permission; or failing to give acknowledgement where permission has been given to reproduce something.

Where colleagues are in receipt of offensive, unacceptable content via social media in a work context, this should be reported to a relevant line manager immediately. Offensive or threatening posts received on personal, private social media accounts should be reported to the service provider and the police.

3.8 Employee personal use of social media at work

The University IT and Communications Facilities Acceptable Use Policy applies to the personal use of social media by employees at work. The University permits only limited private use of social media on University IT systems from University and personal devices for non-university purposes. However, this should not normally be carried out in work time; i.e. should be limited to lunch or other breaks. Where excessive use, interfering with relevant duties, is proven, the University may take disciplinary action.

3.9 Social media and public interest disclosure

Where an employee wishes to release information that may be considered as a Public Interest Disclosure (“Whistle Blowing”), the University’s Public Interest Disclosure Policy must be initiated in the first instance before any action is taken through social media.

4. SCOPE

4.1 This policy applies to

- All employees and to all social media communications which directly or indirectly represent the University.
- Employee use of University social media accounts in the course of their work for the University

- Personal use by colleagues of social media that contains comments about the work of University or their colleagues' work
- Personal use of social media by colleagues, that impacts on University's operational, legal or reputational liabilities
- Casual workers, including external examiners and agency workers engaged on University business
- Students, contractors, suppliers, University partners and external researchers and visitors who are issued with login credentials to manage or post content to University social media accounts on behalf of the University.

4.2 The scope of this policy includes use of social media for promotional, learning, teaching and research activities and for private use that impacts on the University.

Student personal use of social media is out of scope of this policy. However, student use of social media that breaches relevant University policies, such as the Harassment and Bullying Policy for students, may be subject to investigation and action under the Student Discipline procedures for investigating non-academic disciplinary offences.

4.3 Where the Policy applies

This policy applies to online communications posted at any time and from anywhere, whether to an individual, a limited group or the world.

As the University operates internationally, through its campuses in Dubai and in Malaysia and through arrangements with partners in other jurisdictions the remit of the policy shall pay due regard to non-UK legislation that might be applicable.

5. LINES OF RESPONSIBILITY

Colleagues designated as managers of University social media accounts, or with responsibility for organising use of social media for University purposes are responsible for

- undertaking induction and refresher training in social media
- following the objectives set out in section three
- using social media in line with recommended standards and guidelines.

The Secretary of the University has senior management accountability and oversight of measures to ensure that University social media use complies with the University's legal obligations and duties of care to students, staff and other stakeholders.

The Director of Marketing and Communications is responsible for recommending University strategy for use of social media for promotional purposes and liaising with the responsible officers identified in this policy and other relevant staff to develop standards and guidelines to support its effective use. The Director is responsible for approving the creation of all University social media accounts used for marketing and communications purposes aimed at enhancing the University reputation and brand and will maintain a record of all such University social media accounts.

Each Head of School and Director of Professional Service is responsible for approving the creation of all University social media accounts set up by

their School/Service for learning, teaching and research purposes and will maintain a record of all such University social media accounts.

All Heads of Schools and Directors of Professional Services are responsible for promoting and implementing the policy within their business areas.

The Student Learning Experience Committee (SLEC) is responsible for developing and promoting policy and guidance for use of social media in learning and teaching.

The Research and Knowledge Exchange Board (RKEB) is responsible for developing and promoting policy and guidance for use of social media in research projects.

The Director of Governance and Legal Services is responsible for oversight of incident and complaints handling.

The Director of Human Resources Development is responsible for implementing, monitoring and supporting, relevant human resources policies and procedures, including investigations and action arising from investigations in line with Grievance, Disciplinary and Bullying & Harassment Policies.

The Academic Registrar is responsible for investigating complaints made against students under this policy.

The Digital Marketing Officer is responsible for recommending policy and guidance on effective use of social media for marketing and public engagement.

The Head of Heritage and Information Governance is responsible for ensuring that all information governance policies and procedures take account of relevant risks and issues relating to the use of social media, and for providing advice to colleagues and students.

The Director of Information Services is responsible for ensuring that centrally managed IT systems and services support the responsible and secure use of social media.

6 MONITORING AND EVALUATION

The Director of Governance and Legal Services will monitor the effectiveness of this policy by maintaining a comprehensive record of incidents and complaints relating to social media, liaising with the Director of Human Resources Development and the Academic Registrar to capture relevant information.

The Director of Governance and Legal Services will make an annual report to the Secretary's Board on compliance with the policy.

The Director of Marketing and Communications and the Director of Governance and Legal Services will report legal and reputational risks relating to social media to the Risk and Project Management Strategy Group and will monitor the effectiveness of this policy in contributing to the mitigation of these risks.

Social media related incidents involving loss or compromise of personal data or other confidential information will be reported to the University Information

Governance and Security Group in accordance with the remit of the group to review relevant information security incidents and recommend actions where necessary to strengthen information security controls.

7 IMPLEMENTATION

The Secretary of the University is accountable for the implementation of this policy. The University will ensure that implementation of this policy is supported by effective procedures, guidance and appropriate communications, training and awareness raising measures, applicable to all employees; and to any contractors or others delegated to contribute to University social media accounts.

The marketing team within Marketing and Communications will lead the provision of guidance, induction and refresher training for colleagues authorised to use official social media accounts for promotional purposes.

The Centre for Academic Leadership and Development will lead the provision of guidance, induction and refresher training for colleagues authorised to use social media for learning, teaching purposes and research.

The Director of Governance and Legal Services and the Head of Heritage and Information Governance will provide training and guidance on legal, e-safety, data protection, privacy and information security aspects of social media.

8. RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

8.1 University Policies and procedures

This policy should be read in conjunction with the following University policies, which are reviewed and updated as necessary to meet the University's business needs and legal obligations.

For all members of the University community:

- IT and Communications Facilities Acceptable Use Policy
  http://www.hw.ac.uk/documents/it-communications-facilities-acceptable-use.pdf
- Our values
  http://www.hw.ac.uk/about/careers/culture/our-values.htm
- Policy on Intellectual Property, Confidential Information and Commercialisation
  http://www1.hw.ac.uk/hr/p_intellectual_property.php
- Public Interest Disclosure Policy
  http://www.hw.ac.uk/services/docs/publicinterestwhistleblowingprocedure.pdf
- Information Governance and Records Management Policy
  http://www.hw.ac.uk/documents/information-governance-records-management-policy.pdf
- Data Protection Policy
  http://www.hw.ac.uk/documents/heriot-watt-university-data-protection-policy.pdf
- Information Security Policy Framework

http://www.hw.ac.uk/documents/information-security-policy-framework.pdf

- Policy and Procedure for Approving, Monitoring and Reviewing Personal Data Processing Agreements
  http://www1.hw.ac.uk/archive/docs/personal-data-approval-policy.pdf

- Secure use of confidential data on portable media: policy and procedures
  http://www1.hw.ac.uk/reference/confidential-information-on-portable-media-policy.pdf

- Information Security Incident Management policy and procedures
  http://www.hw.ac.uk/documents/information-security-incident-management.pdf

For employees:

- Disciplinary Policy
- Grievance Policy
- Harassment and Bullying Policy

All published at http://www.hw.ac.uk/services/human-resources-policies.htm

- Safeguarding Policy [under development]
- Guidance for hiring managers, including global platform appointments and our Equality and Diversity commitments
  https://intranet.hw.ac.uk/ps/hrd/recruitment/Pages/About-iRecruit.aspx
- Social media guidelines
  Appended to this policy

For students:

- Harassment and Bullying Policy and procedures for Students
  http://www.hw.ac.uk/documents/anti-harassment.pdf
- Student Discipline Policy and procedures
  http://www.hw.ac.uk/students/doc/discguidelines.pdf

8.2 Legal Requirements and external standards

This policy has been developed to comply with U.K. and Scottish law and other relevant law in all jurisdictions in which the University operates.

Legislation that places specific obligations on organisations and individuals in relation to online communications includes, but is not limited to:
Computer Misuse Act 1990
Copyright, Designs and Patents Act 1988
Data Protection Act 1998
Equality Act 2010
Environmental Information (Scotland) Regulations 2004
Freedom of Information (Scotland) Act 2002
Human Rights Act 1998
Privacy and Electronic Communications Regulations 2003
Regulation of Investigatory Powers Act 2000
Regulation of Investigatory Powers (Scotland) Act 2000

All current UK Legislation is published at http://www.legislation.gov.uk/

This policy is based on best practice guidance including the following:

Joint Information Systems Committee JISC Legal:
Social Media for Staff Policy Template (10 February 2014)
http://www.jisclegal.ac.uk/ManageContent/ViewDetail/ID/3443/Social-Media-for-Staff-Policy-Template-10-February-2014.aspx

Advisory, Conciliation and Arbitration Service
(ACAS) Guidance on Social Media
http://www.acas.org.uk/index.aspx?articleid=3375

Universities and Colleges Information Systems Association (UCISA) Social Media Toolkit
http://www.ucisa.ac.uk/~/media/Files/publications/social_media/Social_media_toolkit.ashx

University of York: social media guidelines, October 2012

University of London: social media policy, October 2013

9. DEFINITIONS

Information	The definition of information includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, posted onto intranet or internet sites or communicated using social media.
Confidential information	The definition of confidential information can be summarised as: ▪ Any personal information that would cause damage or distress to individuals if disclosed without their consent. ▪ Any other information that would prejudice the University's or another party's interests if it were disclosed without authorisation.
Personal data	Data which relate to a living individual who can be identified (a) from that data, or (b) from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Social Media	Social Media services are "websites and applications that enable users to create and share content or to participate in social networking." – Oxford Dictionaries This policy refers to external social media services-those hosted on servers over which the University has no control. This includes proprietary social networking sites and platforms such as Facebook, LinkedIn, Twitter and Instagram; Skype, collaboration services such as Wikipedia, YouTube and Flickr.
Social media organiser	A person who sets up or administers a University social media account in the course of University work. This could be a tutor creating a social media account to set up a discussion group for students, an administrator using social media to engage with pre-enrolment students, or a researcher setting up a wiki site for public engagement and collaboration.
University social media account	Any social media account created by or on behalf of the University as a corporate body or a University School or Professional Service for communication to support the University's mission. University social media accounts will be clearly identified with the University branding and logo in line with the Style Guide. Authority to create a University social media account is subject to the lines of approval set out in this policy.
University social media content provider	In the context of this policy, the definition includes academic and professional services employees and any contractors, students or other people linked to the University who have been given delegated approval to contribute University content for a University social media account, whether on a paid or voluntary basis.
Social media users	People making use of a social media service. This might include academic and professional services staff, students, those linked to the institution through business engagement or community engagement, and members of the public in general.
Information Security Management	"That part of the overall management system based on a business risk approach to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organisational structure, polices, planning activities, responsibilities, practices, procedures, processes and resources." BS ISO/IEC 27001: 2013: Information Security

10. FURTHER HELP AND ADVICE

For advice on using social media in learning, teaching and research:

Centre for Academic Learning Development
+44 (0)131 451 3789
academicdevelopment@hw.ac.uk

For advice on making the most of social media and digital communications channels for promotion and marketing:

Digital Marketing Officer
Marketing and Communications
webeditor@hw.ac.uk
+44 (0)131 451 8272/3523

For advice on any aspects of human resources policy issues in relation to social media:

Human Resources Services
Telephone: 0131 451 3022
hr@hw.ac.uk
https://intranet.hw.ac.uk/ps/hrd/Pages/Who's-Who-in-HRD-.aspx

For advice on any aspect of data protection and information security:

Heritage and Information Governance
Telephone: 0131 451 3219
Email: hig@hw.ac.uk

11. POLICY VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
11.3	22.08.2016	University Executive	Minor changes to draft 15/07/2016 on recommendation of the Secretary's Board meeting of 05/07/2016