HERIOT
WATT
UNIVERSITY

Guidelines

Social Media Policy for employees and contractors

GUIDELINES

HERIOT-WATT UNIVERSITY

GUIDELINES TO SUPPORT
SOCIAL MEDIA POLICY FOR EMPLOYEES AND CONTRACTORS

CONTENTS

1. INTRODUCTION

Some colleagues work in roles that involve using official Heriot-Watt social media accounts set up to communicate on behalf the University.

Many colleagues and postgraduate students may use social media in private life. They may also use social media in an individual professional capacity to share knowledge and expertise, collaborate with members of the wider academic community, to contribute to discussion and debate in academic and professional life and for professional networking and career development.

These guidelines should be read in conjunction with the Social Media Policy for Employees and Contractors. They aim to provide detailed guidance on the policy and related issues of reputational risk, privacy, data security and e-safety.

2 GUIDELINES

2.1 Setting up new University branded social media accounts and platforms

The Director of Marketing and Communications has strategic oversight of University social media accounts used for promotional purposes. The Director of Marketing and Communications will approve the creation of and maintain a record of all University branded social media accounts used for these purposes. Heads of Schools will approve the creation of and maintain a record of social media accounts created to support learning, teaching and research. Where a particular School or Service believes they require additional accounts or platforms, the Marketing and Communications team should be notified and consulted in order to review any user agreements, ensure correct use of branding, and advise on standard procedures around security, passwords and content filtering.

2.2 Promoting the University

Colleagues whose roles involve communications with the public may contribute to the University’s social media activities, for instance by running an official University social media account or contributing to blogs and image sharing sites. Colleagues need to be aware at all times that, while contributing to the University's social media activities, they are representing the University.

The same standards and safeguards apply to University communications using social media as any other channel. Colleagues in Marketing and Communication can provide professional support and guidance to members of the University to allow them to make the most effective use of social media to connect and engage with our diverse audiences. Details of the centrally managed social media accounts can be found here: http://www.hw.ac.uk/about/contact/social-media.htm

2.3 Enhancing academic engagement

The University wishes to encourage the use of appropriate social media technologies as part of its teaching and learning provision. The University also recognises the value of social media in promoting and disseminating research, contributing to academic debate and public engagement. Where a research project involves the use of social media to generate research data e.g. by participating in an online community, using social media to recruit or interact with data subjects or analysing social media content, Principal Investigators need to consider the ethical and privacy implications of the research when developing proposals. If colleagues wish to use external social media services to process sensitive personal data or other confidential information for learning, teaching or research, the organiser or Principal Investigator must seek advice from colleagues in Heritage and Information Governance at an early stage so that risks can be identified and properly managed.

2.4 Social media and employee recruitment

The University is committed to fair, open and accountable employee recruitment and selection procedures.

For some jobs, a successful track record of using social media in professional life may be one of the requirements of the role. Examples may include academic or professional service roles that involve using social media as a platform for public engagement. In recruiting academic roles requiring an international research profiles it is legitimate to undertake online searches of research publication gateways, such as Google Scholar, to verify evidence of publication and citations. However, this must be made clear to applicants in the job postings and also be undertaken with care to avoid the risk of unconscious bias.

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 search applicants' public social media profiles only where this is directly relevant to an applicant's skills or claims to check facts or information already disclosed by the applicant. However, Hiring Managers will not make selection decisions based solely or mainly on any information obtained that has not already been disclosed by the applicant during the application process. The Hiring Manager should document the review and any recommendations made as a result of the review in iRecruit, print and scan the page containing social media content reviewed and either attach it to the applicant record in iRecruit or forward the copy to Human Resources Development with any ancillary recruitment records.

Recruiting managers need to be aware that making searches or checks of candidates' social media activities in their personal or private lives as part of the selection process presents significant risks of breaching Equality, Human Rights and Data Protection laws. For this reason, failure to adhere to this Policy may result in disciplinary action. Searches via social media present the risk that managers would gain access to information that is not relevant to the criteria for the job, and could put some candidates at risk of discrimination. Research over social media may reveal information about applicants' protected characteristics such as age, gender, sexual orientation, marital status or religion. Applicants may not have social media accounts so the manager would not have access to equivalent information about all candidates.

Even if an individual has shared personal data online in a public forum, they retain rights in relation to their personal data and private life. Organisations may be vetting individuals on the basis of information about them posted online that may not be accurate. If an organisation wishes to use that data, the use must be fair and lawful and the individuals concerned must be made aware of how the organisation is using their data. Individuals have the right to make a data subject access request to see what online searches organisations have carried out about them as part of a recruitment process. This is why details of the review and a copy of the social media content reviewed must be documented as part of the recruitment record.

2.5 Maintaining ethical boundaries

All colleagues have a particular responsibility to observe the ethical boundaries of the professional/academic/student relationship. To avoid conflicts of interest colleagues need to exercise caution in using their social networking accounts to "befriend" students or colleagues who are in their management line for social purposes.

2.6 How public and private use of social media interact

Heriot-Watt University respects privacy and understands that many colleagues use social media in their private lives. However, personal communications likely to have a negative impact on the University’s reputation are within the scope of the University’s Social Media policy.

Wherever possible, it is best practice to maintain separate social media accounts for professional and private life.

Even so, colleagues need to be aware that personal information, opinions or views posted in a private capacity may adversely affect other people's perceptions of the user in a professional context and may damage the University if they are recognised as being one of our employees. Social media is not confidential communication and is frequently copied and/or re-posted by others. Although it is possible to take down information you have posted online, other users may have already republished it elsewhere. Information, once published online, may remain in the public domain indefinitely.

2.7 Maintaining privacy

By definition, using social media platforms involves publishing personal data. This is any information that could be used to identify a particular living person. Colleagues who use social media in the course of their work for the University therefore need to consider the privacy and data protection aspects of their activity, and in particular, whether it involves posting personal data on public sites. Colleagues need to ensure that that they collect only the minimum amount of personal data necessary to conduct the relevant University activity and that the data is adequate and relevant to fulfil the purpose for which it was collected.

The University is legally accountable for any breaches of privacy and data security by colleagues who use social media services to process personal data for University purposes. External social media services are hosted on servers over which the University has no control. The service providers require organisers and users to sign up to standard terms of service and privacy policies and decline to enter into the University’s Data Processor confidentiality agreement, which would normally form part of the contractual agreement with external service providers. In addition, most external social media service providers hold users’ personal data on servers that are hosted outside the European Economic Area (EEA). This means that additional safeguards need to be in place to ensure that personal data is processed lawfully.

The University relies on the fact that users who sign up to join external social media services and chose to follow or post content to University social media sites have given their free and informed consent for their data to be held and seen, in accordance with the privacy settings that they have enabled.

In order to ensure that individuals' personal data is always processed in accordance with their rights, managers of social media accounts need to ensure that site privacy settings are appropriate for the purpose, content and intended audience and explain these to users. In this way, people who chose to join a University site will understand what will be done with their personal data and who else can see it.

Colleagues need to avoid using social media for University discussion and collaboration, where this involves asking participants to share sensitive personal data, for instance relating to physical or mental health, or any other information that could cause damage or distress to individuals if disclosed without their consent.

If colleagues wish to use external social media services to process sensitive personal data or other confidential information for learning, teaching or research, the organiser or Principal Investigator must seek advice from the Heritage and Information Governance at an early stage, for instance as part of the ethical approval process, so that risks can be identified and properly managed.

When setting up closed social media groups organisers need to obtain each participant's explicit consent to share their data with the group. Organisers are responsible for ensuring that group privacy settings are managed to restrict access to members only and that members understand the need to maintain confidentiality as part of induction covering data protection issues and privacy setting checks (e.g. use of cookies, usage monitoring) on social media tools before registering to use them.

2.8 Promoting e-Safety

The University takes e-safety and its duty of care seriously and will do all that it reasonably can to ensure that learning and working environments, including social media, are safe for colleagues and learners.

Administrators, academic heads and course leaders who use social media in learning and teaching share responsibility for inducting learners in e-safety before permitting access to University social media accounts.

Where colleagues are working with younger and/or more vulnerable learners, course leaders need to consider extra safeguards such as moderating content prior to publication.

All users need to be aware of the privacy, fraud and reputational risks associated with using social media sites to share private information online and make appropriate use of privacy settings to control access to information they may post online. For instance, cyber criminals may use information in social media posts about users' dates of birth, family members, pets, favourite music, film or sports teams to try to guess passwords or otherwise compromise accounts.

2.9 Keeping networks and data secure

As with other online activity, all users of social media need to take appropriate action to avoid compromising the security of University IT systems. Users should beware of viruses and phishing attempts when using third party applications and be cautious in opening attachments or links to URLs even when they appear to come from trusted sources.

Colleagues are responsible for ensuring that passwords and other access controls for University social media accounts are of adequate strength and kept secure. All passwords should be at least 8-10 characters long and contain a mixture of upper and lower case letters, numbers or symbols. 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 user. 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 access work 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.

The University will regularly review and update security software up to date and take other appropriate security measures to prevent accidental or malicious access of IT systems and social media accounts. Usage of University IT and Communications Facilities may be logged for the purposes of system management, to protect systems and also to investigate misuse, in accordance with the University Information Security Incident Management Policy.

2.10 Ensuring accessibility for all users

Colleagues who manage social media accounts in their work for the University are responsible for ensuring that, where a reasonable adjustment is possible, these services are accessible by users with disabilities and that the technologies used comply with general accessibility standards. Colleagues who set up or use social media accounts for work need to consider any accessibility issues inherent in the use of that technology, to ensure that the delivery platform provides an accessible learning experience to all users.

2.11 Protecting Intellectual Property Rights (IPR)

Heriot-Watt University values its intellectual property and respects the intellectual property rights of third parties. Colleagues are responsible for consulting the service's terms and conditions to identify any IPR policy that may conflict with the University's Policy on Intellectual Property, Confidential Information and Commercialisation.

Colleagues who manage University social media accounts are responsible for reminding users of the University's IPR policy and of their obligations in relation to the clearance of IPR-protected material. Members of the University community who post content to University social media accounts need to exercise caution when referring to or copying content and images produced by third parties to avoid the risk of infringing intellectual property rights. Users are responsible for checking terms of service and copyright notices and for obtaining permission to use and acknowledging third party content.

Users of social media need to take particular care to avoid publishing confidential information into the public domain, e.g. information that relates to a potential patent application or is otherwise commercially valuable, or discussions about business plans or partnership activities that have not been announced or published by the University.

2.12 Maintaining business continuity

Before adopting the use of an externally provided social media service for University information, the organiser needs to consider the stability and security of that service, the loss, damage and/or disruption that would be caused by failure of the service, and the corresponding benefit that using the service brings.

Organisers of externally hosted social media services need to ensure that any business information that needs to be retained and referred to for operational purposes is copied onto secure University IT systems, which are appropriately backed up. In this way if the information is no longer accessible from the social media platform, the University will retain accessible, reliable records as long as required in accordance with the University's records retention policies.

2.13 Social media and information rights

Social media organisers need to be aware that information processed for University business using social media is potentially disclosable under the Freedom of Information (Scotland) Act 2002. Individuals whose personal data is processed for University purposes on social media also have the right to request access to their own personal data under the Data Protection Act, 1998.

Individuals may also use social media to request information from the University under Freedom of information and Data Protection laws.

All requests for information that cannot be provided in the normal line of business need to be referred promptly to colleagues in Heritage and Information Governance who will coordinate an appropriate response.

2.14 Managing incidents, reporting inappropriate content and handling complaints

The University has a responsibility to investigate and to take appropriate action to deal with all instances of misconduct involving members of the University community that are drawn to its attention, whether they take place online or face to face. Examples of inappropriate use of social media which may incur disciplinary action fall into four main categories:

- Cyber bullying and discriminatory behaviour
- Breach of confidentiality
- Defamation and other conduct that brings the University into disrepute
- Breach of copyright

Examples are detailed in section 3 of the Policy.

Any breach of this policy could lead to disciplinary action, the outcome of which may include dismissal for Gross Misconduct. Where a breach of this policy is reported to the University, the relevant University officers will act immediately to investigate the incident and take appropriate steps to mitigate its impact. Anyone may report an incident to the University. This should be directed immediately to the generic University email and contact point for reporting concerns about inappropriate use of University social media sites, webeditor@hw.ac.uk or the relevant managers listed below.

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.

The Director of Governance and Legal Services (DGaLS) has overall responsibility for managing breaches of policy and for investigating complaints from members of the public.

The Head of Heritage and Information Governance will manage the response to social media related incidents involving loss or compromise of personal data or other confidential information.

The Director of Human Resources Development is responsible for managing the processes relating to the investigation of allegations of breaches or complaints involving employees.

The Academic Registrar is responsible for investigating breaches involving complaints involving students.

These officers will and liaise with DGaLS to seek advice on legal issues where necessary and report on outcomes to DGaLS.

3. 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:

For advice on using social media for promotional purposes:

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
+44 (0)131 451 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: +44 (0)131 451 3218/9/3274
Email: hig@hw.ac.uk

4. DEFINITIONS

Confidential information

The definition of confidential information can be summarised as:

- Any personal information in any format that would cause damage or distress to individuals if disclosed without their consent.

- Any other information in any format that would prejudice the University's or another party’s interests if it were disclosed without authorisation.

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.

Personal data

Means data which relate to a living individual who can be identified –
(a) from those data, or
(b) from those 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 organiser

A person who sets up or administers a particular social media service 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.

5. GUIDELINES VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
V. 1.2	22 August 2016	Presented to the University Executive	Minor amendments in line with revisions to policy 15/07/2016