Staff Use of Social Media

Purpose and Context

These guidelines are intended to advise and assist members of staff using social media either as part of their professional role at the University or in a private capacity.

Scope

This policy applies to all University staff and to all communications on social media which directly or indirectly represent or impact upon the University, its staff and/or students.

This policy applies to social media communications made at any time, in any language, whether privately or publicly, including outside of normal working hours, and from anywhere, including away from campus, whether to an individual, to a limited group or to the world. For the purposes of this policy, private use of social media means use of social media intended to be shared with a limited number of individuals (such as a private group, or one-to-one communication) but has nevertheless become more generally known or accessible.

---

1   Introduction

1.1   The use of social media is an important means of communication both to enhance the profile of the University and the professional profile of individuals. These guidelines are intended to advise and assist members of staff using social media either as part of their professional role at the University or in a private capacity where boundaries between work responsibilities and home life can get blurred. They are not intended to restrict scholarly, academic or pedagogic use of the media. Neither are they intended to restrict what members of staff say or do in a personal capacity, nor prevent members of staff from expressing critical comment.

1.2   The University does not restrict the personal use of email or internet so long as this does not interfere with someone's ability to carry out their work effectively. However, the University does have responsibilities to maintain the security of its systems and information and to protect its reputation. Individual members of staff have a contractual obligation not to misuse the University's resources and not to take action that brings the University into disrepute. Members of staff also have a responsibility to ensure that they do not breach the Disciplinary Rules of the University. These guidelines are designed to assist staff in ensuring that they have access to social media without inadvertently breaching conduct rules or the University's computing regulations.

1.3   Unfortunately, some organisations or individuals may make abusive use of these communication methods. These guidelines also provide some basic

guidance on protecting your privacy and advice on what you can do if you are subject to harassment or bullying via this form of communication.

2   Guidance for members of staff who use social media as part of their role

2.1   This section applies to University staff who create or contribute to blogs, wikis, social networks, virtual worlds, social networking sites or any other kind of social media.

2.2   Members of staff using this media as part of their job are representing the University. You should therefore make clear that you work at the University, use your real name and be clear about your role. The lines between public and private, personal and professional can become blurred in online social networks. If you are identified as a member of the University you need to ensure that your content and tone is consistent with your role at work.

2.3   As with all communication you make on behalf of the University there is a reasonable expectation that you are respectful to others. You should therefore avoid spam or remarks that are off-topic and must not post offensive comments.

2.4   All statements you make must be true and not misleading. If you speak about other education providers make sure what you say is factually correct and that it does not disparage them. Avoid unnecessary or unproductive arguments. If you make an error, acknowledge your mistake, and correct it. If you modify content that was previously posted, for example editing a blog, make it clear you have done this.

2.5   In an academic context it is inevitable that there will be debate. You should feel free to comment on your area of expertise but ensure that you are not disclosing any confidential information regarding the University and maintain standards required in Data Protection legislation in discussing other people. When disagreeing with others' opinions, however heated the debate, be polite. What you say and how you disengage with a debate reflects on you as a professional and on the University.

2.6   In line with usual standards about disclosure of information you must not publish or report on conversations that are meant to be private or internal to the University unless you seek prior permission. You must not publish or report on any items of communication of the University, unless this is already in the public domain, without seeking permission. You must not post any photographs of people unless you have their permission (any photographs of children and young people under the age of 16 should have parental permission).

2.7   Do not comment on anything related to legal matters, litigation, or any parties the University may be in dispute with.

2.8   Do not comment on anything that may be considered a crisis situation.

2.9   Any use of the University's equipment/or server is covered by the University's Computing Regulations and the JANET Policy on Acceptable Use. You should ensure that you comply with these requirements at all times. The standards that apply to staff conduct in general also apply to on-line activity.

2.10   If you are in any doubt about what you want to publish, please seek further guidance from your manager or the Marketing and Communications Office.

3   Using Social Media in a Personal Capacity

3.1   If you access social media at work or you use your University email account (even on your home computer) you must ensure that you comply with University's Computing Regulations, the JANET Policy on Acceptable Use and the University's guidance on Conduct relating to Email and Internet Use. You should ensure that you know what these requirements are and you abide by them at all times.

3.2   When using social media in a personal context, members of staff are still expected to uphold University values, respect other employees, students and stakeholders, and protect confidentiality, privacy and security.

3.3   Your conduct outside of work will affect your employment if your conduct could be said to bring the University into disrepute or where your conduct outside of work compromises your ability to carry out your role effectively.

3.4   In line with usual standards about disclosure of information you must not publish or report on conversations that are meant to be private or internal to the University unless you seek prior permission. You must not publish or report on any items of communication of the University, unless this is already in the public domain, without seeking permission. You must not post any photographs of people unless you have their permission (any photographs of children and young people under the age of 16 should have parental permission).

3.5   Beware of breaching Data Protection requirements, for example, if you blog about your day at work and say "*Frank was off sick today*" you may have breached the Data Protection Act requirements about the use of sensitive data.

3.6   Some people may use the social media as a means of expressing their discontent about work or their work colleagues. This is not advised as it is not a productive route to resolve any grievance you may have. If you disagree with the impact that a University policy or procedure has on you then you are encouraged to pursue this through the University's Grievance Procedure. Clearly, you are free to express views about the University and will not be liable to any breach of the disciplinary rules so long as you ensure that a) you make it clear you are "speaking" from a personal perspective, b) your statements are true and can be substantiated and c) you are not breaching confidentiality or other legal requirements.

3.7   You should not refer to other named members of staff, students, contractors or clients unless you have their express permission. Neither should you create "personas" attached to staff, students, contractors or clients where this will lead to the identification of the person you refer to. To do so may lead to complaints against you relating to a breach of Data Protection and/or harassment.

3.8   Nothing in the above guidance should be interpreted as a restriction on an individual's right to pursue action under the Public Interest Disclosure Act, commonly referred to as "whistleblowing". It should also be noted that disclosures on social networking sites are covered within the Act and therefore

you should ensure you have legal immunity prior to a post or other communication.

3.9 Staff are reminded that other members of staff and/or students may see their activity on social media. Even when privacy settings are used, there is no guarantee that posts cannot be copies or shared.

3.10 Personal use of social media during working hours should not be excessive or interfere with a member of staff's role or commitment to the University. Local rules may also apply to the use of personal social media during working hours. The University reserves the right to restrict access to social media sites if it deems it necessary to do so.

3.11 If you have any concerns regarding your use of the social media and how this affects your employment you should consult your trade union representative or Human Resources.

4 Cyberbullying

4.1 Cyberbullying is where someone, or a group of people, threaten/harass someone using social media, email or mobile phone. Where staff are subject to such practice they are advised to respond as follows:

   a) if the originator of the material is a member of staff you should consider whether this can be resolved under the informal processes within the Dignity at Work Procedures. If not, you should make a complaint in accordance with the formal procedures of the Dignity at Work Procedures. The University reserves the right to investigate and manage any complaints under the disciplinary procedures where a breach of conduct rules is alleged.
   b) if the originator of the material is a student you should report this to your line manager and the matter will be dealt with in accordance with the Students' Disciplinary Procedure.
   c) if the originator of the material is a contractor, client or visitor to the University you should immediately report this to your manager and HR.
   d) if the originator of the material has no connection to the University you should consider reporting the matter to the police.
   e) in all cases you should report this to the website/internet forum requesting that the people naming you are removed as users.

5 Recruitment of Staff

5.1 Personal or private social media activities of prospective staff will not be looked at as part of the recruitment and selection process; however, where a candidate uses social media professionally or has explicitly mentioned the use of social media in their application or CV (e.g. by providing a LinkedIn profile or web address), social media may be reviewed and considered.

6 General Guidance

6.1 Think about your own privacy, check any site's privacy statement to see what you are signing up to and set privacy settings appropriately. Social network

pages, blogs etc. are public. Do not put information on them that you do not want others to see. Once information has been posted it can be very difficult to remove. Even if you unsubscribe from a site the information may continue to remain visible for a long time.

6.2 Some websites will ask you to complete a registration form before you can use them. All companies who collect personal information have to tell you how that personal information will be used. This information is contained in the website's terms and conditions.

6.3 Do not send your bank details to anyone in an email. Legitimate banks and stores will not ask you to do this. Even if you receive an official-looking email that asks for financial details, do not respond.

7 Monitoring

7.1 At the University, there is no routine monitoring of electronic communications although all University web activity is logged, and access to sites which are likely to cause a breach of the Computing Regulations may be blocked. However, the University reserves the right to sanction investigation and inspection of electronic communications, where there is a complaint of an infringement of the regulations or the rules of the University.

8 Reporting issues

8.1 Where members of staff are in receipt, or become aware, of offensive or unacceptable content on or through social media, this should be reported to their line manager in the first instance. Advice may also be sought from Human Resources.

POLICY SIGN-OFF AND OWNERSHIP DETAILS

Document name:	Staff Use of Social Media
Version Number:	V1.4
Equality Impact Assessment:	Completed TBC
Approved by:	Head of HR
Date Approved:	December 2021
Next Review due by:	December 2024
Author:	HR Manager
Owner (if different from above):	Director of Human Resources
Document Location:	https://www.hud.ac.uk/media/policydocuments/Staff-Use-Of-Social-Media.pdf
Compliance Checks:	HRG regularly review to ensure compliance
Related Policies/Procedures:	

REVISION HISTORY

Version	Date	Revision description/Summary of changes	Author
V1.1	October 2016	Formatting updates (minor amends not requiring committee approval)	HR Manager
V1.2	November 2019	Formatting updates (minor amends not requiring committee approval) and transference to new template	HR Manager
V1.3	April 2021	Formatting updates (minor amends not requiring committee approval) and transference to new template	HR Manager
V1.4	December 2021	Formatting updates (minor amends not requiring committee approval)	HR Manager