Social Media
Policy and Procedure

1 INTRODUCTION

Whilst the University expects its employees and staff to comply with this policy, it does not confer contractual rights or form part of any contract of employment and may be amended by the University or replaced at any time following appropriate consultation and negotiation with recognised trade unions. Breach of this policy may be addressed via the University's Disciplinary Policy and Procedure and Code of Conduct.

This policy will be reviewed by the Human Resources department on a 3-year basis or amended in response to changes in future legislation and/or case law, as well as in response to changes in social media technology and capabilities.

2 OWNERSHIP

The Human Resources department owns and manages this policy on behalf of The University of Northampton.

3 ORGANISATIONAL SCOPE

This Social Media policy is a corporate policy and applies to all employees, workers and agency workers, as applicable, of The University of Northampton including any wholly owned subsidiaries, unless an alternative policy exists, subject to any qualifying conditions.

4 POLICY STATEMENT

4.1 This policy sets out a framework to promote effective use of social media with the purpose of maintaining a safe, professional environment and protecting the interests of the University and all members of the University community.

4.2 The University 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 staff about acceptable and unacceptable use of social media, in line with its wider policies such as the Acceptable Use Policy and the Code of Conduct. Any breach of this policy could lead to disciplinary action, up to and including dismissal.

4.3 This policy applies to any professional or personal communications within a social media platform which directly or indirectly reference the University.

4.4 This policy applies to the use of social media by its staff for both business and personal purposes, whether it is in normal work time or not, on University or personal devices, and whether posting on social media using personal or work-related accounts.

4.5 The Policy is not intended to limit or undermine the principles of either free speech or academic freedom, subject to that freedom being exercised within the law.

4.6 For the purposes of this policy, 'social media' includes but is not limited to the examples given in the definitions section below.

5 DEFINITIONS

5.1 **Social Media** – interactive web-based platforms or apps that enable users to communicate instantly with each other; to create or share content in a public forum; or to participate in social networking. There are many types of social media platforms and this is a constantly changing area but some popular ones include:

Type	Explanation	Examples
Social networks	where people can connect to others in some cases based on mutual interests or hobbies	Facebook, Whatsapp, Twitter, LinkedIn Goodreads
Media sharing networks	for sharing photos, videos, and other media	YouTube, Instagram
Discussion forums	for sharing news, views and ideas	reddit, Quora, Digg
Blogging and publishing networks	where people can publish content	WordPress, Tumblr
Review networks	where people leave reviews of businesses which are searchable by others	Yelp, TripAdvisor
Shopping networks	for shopping online	Etsy, Fancy

5.2 **Cyber Bullying** - behaviour displayed through social media communications including (but not limited to) maliciously spreading rumours, lies or gossip about others; using intimidating or aggressive behaviour; posting offensive or threatening comments or content; deliberately mocking an individual with the intent to harass or humiliate them. Cyber bullying may also take place via other means of electronic communication such as email, text or instant messaging.

5.3 **Information** - the definition of information includes, but is not limited 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.

5.4 **Fake news** - False stories that have no basis in fact but are presented as being factually accurate.

6 KEY PRINCIPLES

6.1 The University recognises the benefits that the use of social media can bring to the organisation and to individual staff members; to enhance our ability to communicate and network with colleagues, students and the public. However, it is also essential to recognise and manage the legal, ethical and reputational risks arising from the use of social media. Information, once published online, may remain in the public domain indefinitely.

6.2 Although the University allows staff open access to the internet (and therefore any social media platforms) and email whilst at work, access for personal purposes should be kept to a minimum and should generally be made during agreed breaks from work or outside of work time.

6.3 Staff are encouraged to use university provided communication methods such as email and not personal social media. Where staff intend to use social media as a teaching and learning tool, this should be done in the context and spirit of this policy ensuring the expected standards of behaviour are observed by staff and students at all times.

6.4 The University has no direct control over the information staff choose to disclose on social media platforms. However, staff must remember the need to protect the reputation of the University, their own privacy, the privacy of colleagues and students, and the confidentiality of University information/data in any communications or statements they make available to members of the general public, which includes family and friends outside of the University.

6.5 Staff must be aware of how their posts on social media might be received including any reasonable likelihood that their posts might cause offence, where they have friends or links with students and/or professional contacts through their social media account.

6.6 Staff should also be aware that any digital material posted online could reach a wider audience than would have been expected or intended. Once digital content has been created and shared, the originator will have limited control over its permanence and audience.

6.7 The University acknowledges that staff use social media as a form of professional communication through official University websites and accounts and/or by using the University name and logo. For the avoidance of doubt, all professional communications are covered by this policy.

6.8 Where a private social media account is used which identifies the University, it must be made clear that the account is private to avoid the impression that the views expressed on or through that social media account are made on behalf of the University.

6.9 Unauthorised audio recording of conversations in relation to anything covered in this policy is prohibited. Anyone in breach of this may be subject to disciplinary action.

7 PROCEDURE

Social Media for Work

7.1 Communications on social media must be professional and respectful at all times and in accordance with this policy and procedure. 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, and in accordance with the University's Equality and Inclusion Policy and Procedure and Code of Conduct.

7.2 Comments made by staff specifically in the private UON Facebook group must be professional and respectful to all colleagues and the channel must not be used as a vehicle for airing criticisms against colleagues, faculties or departments.

7.3 Comments made by staff on social media in relation to student matters must remain neutral and student posts should not be liked or retweeted in cases where it may convey favouritism in any way.

7.4 Complaints/requests to specific departments should not be made via the UON Facebook group as they are not monitored by the relevant departments. Instead, staff should visit www.northampton.ac.uk/help accordingly.

7.5 All social media accounts created by University staff members for the official business purposes of the University must comply with the Social Media Code of Practice, available from the Marketing and International Relations department.

7.6 Identification of social media accounts

7.6.1 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 Brand Guidelines, available on the intranet.

7.6.2 Staff must also include a disclaimer on any social media profile when publicly commenting on content related to University business that identifies them as a staff member. An example disclaimer of this kind could read, "views expressed are mine and don't necessarily reflect those of my employer".

7.6.3 Any personal social media account that does not identify an individual as an employee of the University or related company does not need to include a disclaimer if the employee will not be commenting on university related business.

7.7 Security of University social media accounts

7.7.1 Staff who manage a University social media account are responsible for ensuring that passwords are in line with the Password Protocol, ensuring strong passwords that are different from UON system accounts.

7.7.2 Accounts should not be left open and unattended for any period. Staff will be held accountable for messages/uploads etc made from their account (for example if they have shared a password), unless they can evidence that their account has been hacked.

7.7.3 Anyone using a personal device to manage a University social media account 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.

7.8 Intellectual property rights in University social media accounts

7.8.1 The content of University social media accounts created by staff on University business and associated intellectual property rights belong to the University.

7.8.2 Where staff 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.

7.8.3 All staff must ensure that they have permission to share any third party materials, including all images, photographs, text and videos, before uploading them to or linking to them via social media and, where sharing is permitted, should ensure that such materials or shared links are credited appropriately.

7.8.4 In addition, all staff must check the terms and conditions of a social media account and/or website before uploading material to it; by posting material to social media accounts and/or websites, you may be releasing

ownership rights and control of the content.
For this reason, you must exercise caution in sharing information.

7.9 Use of social media in staff recruitment

7.9.1 The University may use social media to promote job vacancies to potential applicants. This will only be done in addition to advertising on the University website to avoid excluding potential applicants who do not use social media.

7.9.2 Staff such as Hiring Managers who wish to use social media to promote a job vacancy need to ensure the link to the vacancy as shown on the University website is included in their post and that their message is consistent with the criteria set out in the University posted advert.

7.9.3 Staff must not provide formal references on behalf of the University for other individuals on social media and/or professional networking websites, as such references whether positive or negative, may be attributed to the University and may create legal liability for both the author and the University.

Social Media for Personal Use

7.10 Use of social media and email for personal purposes while at work should be kept to a minimum and should generally be done during agreed breaks or outside of work time. Where excessive use occurs, interfering with relevant duties, the University may be required to take action under the University's Disciplinary Policy and Procedure.

7.11 All members of staff should be aware of their association with, and responsibilities to the University, and ensure that their personal profiles on social media and related content do not conflict with this policy in relation to use of personal social media accounts nor with their employment contract with the University.

Expected standards of behaviour

7.12 All staff should be aware of the potential impact and permanence of anything that they post online. Therefore, posting anything online that they would not wish to be in the public domain and/or that they would not be willing to say personally to the face of another individual, should be avoided.

7.13 No personal information, including photographs and videos, should be shared on social media without the consent (as defined in GDPR article 4 (ii)) of the individual to whom it relates. Staff should, therefore, never post other staff and/or student's and/or a third party's personal information without their consent.

The Freedom of Information Act 2000 may apply to posts and content that you have uploaded to official University websites, or any other website belonging to a public authority. As such, if a request for such information is received by the University, the content that you have posted may be disclosed.

7.14 When using a University social media account or when using another social media account (including a private one) where the account identifies the University, staff are personally responsible for what they communicate and they must adhere to the expected standards of behaviour set out in this policy and the University's Code of Conduct. If a private account is used, it must be made clear that the account is private and that anything posted through the account is not made on behalf of the University.

Dealing with misconduct

7.15 The University has a responsibility to investigate and take appropriate action to deal with all instances of staff misconduct that are drawn to its attention, whether they take place online or face to face. Misconduct will be dealt with under the University's Disciplinary Policy and Procedure as well as in accordance with any other relevant University policy or procedure such as the Code of Conduct.

7.16 Examples of misconduct related to social media use in a personal or professional capacity which may incur disciplinary action (up to and including dismissal) include:

- Behaviour that could reasonably be perceived to be the cause of another person's distress or discomfort, such as that which could be perceived as threatening, obscene, indecent or hostile, or that which could be considered discriminatory or to constitute bullying (or 'cyber bullying') or harassment, such as by making offensive or derogatory comments; posting images that are discriminatory or offensive, or posting links to such content;

- Breach of confidentiality, such as revealing confidential intellectual property or information owned by the University or another 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, staff and anyone else whose personal data is held by the University, is in contravention of the requirements of the existing Data Protection Act and the General Data Protection Regulation (GDPR). Personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. This includes:

    - sharing the personal data of others
    - posting comments using fake accounts
    - posting comments about somebody online
    - using a person's name without their consent

- Posting indecent images without a person's consent (i.e. 'revenge porn'), in contravention of section 33 of the Criminal Justices and Courts Act (2015);

- Conduct which brings the University into disrepute or which compromises the safety or reputation of colleagues, former colleagues, students and those connected with the University, such as 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;

- Social media content which refers to, or includes, information that is in any way inconsistent with an individual's contractual duties to the University or is in pursuance of unauthorised commercial activities.

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

- Excessive use of social media while at work;

- Generation and sharing of fake news or misinformation;

- Any posting that constitutes a criminal offence.

7.17 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.

7.18 Where an employee wishes to release information that may be considered as a Public Interest Disclosure ("Whistle Blowing") the University's Whistleblowing Policy and Procedure must be initiated in the first instance before any action is taken through social media.

Monitoring

7.19 The University reserves the right to monitor, intercept and review within the law, without further notice, staff activities using its IT resources and communications systems, including but not limited to social media postings, to ensure that its rules are being complied with and such activities are for legitimate purposes.

7.20 The use of social media may be monitored by the University in accordance with the IT Acceptable Use Policy. Where excessive use of social media is suspected, the University may take further action in line with section 7.16 above.

8 ASSOCIATED DOCUMENTS

- BYOD Policy
- Code of Conduct
- Disciplinary Policy and Procedure
- Equality and Inclusion Policy and Procedure
- Freedom of Expression Policy
- GDPR DPA Policy and Procedures
- Password Protocol
- Smart Working & Security Policy
- IT Acceptable Use Policy
- Whistleblowing Policy and Procedure

9 EQUALITY IMPACT ASSESSMENT

An Equality Impact Assessment must accompany this document.

10 VERSION CONTROL

Version Control		**Approval record**	
Author:	Joanna Williams (HR Business Partner)	Approval:	TU Liaison – 6/12/19 UMT – 17/12/19
Date written:	July 2019	Updates:	
Current status:	Approved	Approval of revision	

Record of Amendments			
Date	Version number	Details of Change	Approval
22/07/2019	2	Re-writing extensively to make relevant for the changes that have taken place since 2013 with social media - its scope and use, as well as to update based on changes in legislation.	17/12/19