



BUCKINGHAMSHIRE
NEW UNIVERSITY

EST. 1891



SOCIAL MEDIA POLICY

Contents

Introduction	2
Scope	2
Guidance for employees who use social media as part of their role	3
Using social media in a personal capacity	4
Cyber or Electronic bullying	5
General guidance	5
Monitoring	6
Review	6

Approved by: **Senior Management Team**
Version No. **2.0**
Owner: **Human Resources Directorate**

Date first published: **May-2012**
Date updated: **Jan-2016**
Review Date: **Jun-2018**

This document has been designed to be accessible for readers. However, should you require the document in an alternative format please contact the Academic Quality Directorate.

Introduction

- 1 Bucks New University is committed to making the best use of available technology and innovation to improve communication, interaction and other needs of staff, students and partners.
- 2 The use of social media is an important means of communication both to enhance the profile of Bucks New University (the University) and the professional profile of individuals. This policy is intended to advise and assist employees 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 become blurred. It is not intended to restrict scholarly, academic or pedagogic use of the media. Neither is it intended to restrict what employees say or do in a personal capacity, nor prevent employees from expressing critical comment.
- 3 Employees should not spend an excessive amount of time while at work using social media websites. They should ensure that use of social media does not interfere with their other duties as this is likely to have a detrimental effect on productivity.
- 4 The University does have responsibilities to maintain the security of its systems and information and to protect its reputation. Individual employees have a contractual obligation not to misuse the University's resources and not to take action that brings the University into disrepute. Employees also have a responsibility to ensure that they do not breach the disciplinary rules of the University, Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the organisation, may constitute gross misconduct and lead to dismissal. This policy is designed to assist employees in ensuring that they have access to social media without inadvertently breaching the expected levels of conduct or the University's computing regulations.
- 5 The University's values of clarity, openness, respect and delivery on commitments (CORD) and all current policies concerning employees also apply to the use of social media, these include:
 - a HR policies, particularly; Grievance Procedures and Disciplinary Procedures
 - b Equalities policies, particularly; Dignity at Work Policy – Bullying and Harassment
 - c IT policies, particularly; IT Regulations of Use, Email policy, Statement on Internet Use, Mobile Phone Use Policy, Data Protection
 - d Communication policies, particularly relating to the University's Style Guide and Brand Guidelines.

Scope

- 6 This policy applies to all employees working at or on behalf of the University

Guidance for employees who use social media as part of their role

- 7 Employees using social media as part of their role are representing the University, and should therefore make it clear that they work at the University, use their real name and be clear about their role. If an employee is identified as a member of the University they need to ensure that their content and tone is consistent with their role at work.
- 8 The University website provides the opportunity for individuals to set up communities which enable employees and students to share ideas and content such as files and blogs. Employees are therefore encouraged to use the University website for online communication with students. Employees should consider carefully whether there is need to set up networks in external social media, bearing in mind the need to make sure that content is updated regularly and the need to adhere to the University's policies. Content may therefore be better channelled through the University's official groups.
- 9 Employees should not set up sites, groups or pages that purport to be official University sites, groups or pages or use the University's branding without the permission of the Marketing and Student Recruitment Directorate, whether they are acting independently or on behalf of third parties.
- 10 The University's virtual learning environment should be used for online course-related materials.
- 11 As with all communication made on behalf of the University it is expected that employees are respectful to others. Employees should therefore avoid spam or remarks that are off-topic and must not post offensive or discriminatory comments.
- 12 All statements made must be true and not misleading. If an employee speaks about other educational providers they should make sure that it is factually correct and that it does not disparage the provider. Unnecessary or unproductive arguments should be avoided. If an employee makes an error, the mistake should be acknowledged and corrected. If an employee modifies content that was previously posted, for example editing a blog, they should make clear that they have done this.
- 13 In an academic context it is expected that there will be debate. An employee should feel free to comment on their area of expertise, but ensure that they are not disclosing any confidential information regarding the University and maintain standards required in Data Protection legislation when discussing other people. Even when disagreeing with others' opinions, however heated the debate, employees should be polite. What an employee says and how they engage and disengage with a debate reflects on them as a professional and on the University.
- 14 In line with usual standards about disclosure of information employees must not publish or report on conversations that are meant to be private or internal to the University unless they seek prior permission. Employees must not publish or report on any items of communication about the University, unless this is already in the public domain, without seeking permission.
- 15 Employees must not post any photographs of people unless they have their permission (any photographs of children and young people under the age of 16 should

have parental permission). The University does hold an archive of photographs that have been approved for use and the Marketing and Student Recruitment Directorate should be contacted for further details.

- 16 Employees should not comment on anything related to legal matters, litigation, or any parties the University may be in dispute with or anything that may be considered a crisis situation.
- 17 Employees should consult the Marketing and Student Recruitment Directorate when setting up or maintaining social media accounts or websites.

Using social media in a personal capacity

- 18 If an employee accesses social media at work or they use their University email account (even on their home computer) they must ensure that they comply with the University's *IT Regulations of Use Policy*, *Email Policy*, *Statement on Internet Use* and *Mobile Phone Use Policy*.
- 19 An employee's conduct outside of work will affect their employment if their conduct could be said to bring the University into disrepute or where their conduct outside of work compromises their ability to carry out their role effectively or affects work colleagues.
- 20 As stated in 15 and 16 above the same guidance applies for personal use i.e. in line with usual standards about disclosure of information employees must not publish or report on conversations that are meant to be private or internal to the University unless they seek prior permission. Employees must not publish or report on any items of communication about the University, unless this is already in the public domain, without seeking permission. Employees must not post any photographs of people unless they have their permission (any photographs of children and young people under the age of 16 should have parental permission).
- 21 Employees should beware of breaching data protection requirements, for example, if an employee blogs about their day at work and states that "Joe Bloggs was off sick today" they may have breached the Data Protection Act requirements about the use of sensitive data.
- 22 Employees are discouraged from using social media to express discontent about work or their work colleagues. This is not appropriate as it is not a productive route to resolve any issues they may have and it may also be breaching the University's *Dignity at Work Policy*. If an employee has a complaint they are encouraged to discuss this with their manager or to pursue this through the University's *Grievance Procedures*.
- 23 Clearly, employees are free to express views about the University and will not be liable to any breach of the disciplinary rules so long as they ensure that:
 - a they make it clear that they are "speaking" from a personal perspective
 - b that their statements are true and can be substantiated, and
 - c they are not breaching confidentiality or other legal requirements

- 24 An employee should not refer to named employees, students, contractors or clients unless they have their express permission. Neither, should they create “personas” attached to employees, students, contractors or clients where this will lead to the identification of the individual referred to. To do so may lead to complaints against the employee relating to a breach of data protection and/or harassment.
- 25 Nothing in the above guidance should be interpreted as a restriction on an employee’s right to pursue action under the Public Interest Disclosure Act, commonly referred to as “whistle blowing”. It should also be noted that disclosures on social networking sites are covered within the Act and therefore employees should ensure they have legal immunity prior to a post or other communication. Please refer to the University’s *Raising Issues of Concern (Whistle Blowing) Policy*.
- 26 If an employee has any concerns regarding the use of social media and how this affects their employment they should consult their line manager or HR Business Partner or their trade union representative

Cyber or Electronic bullying

- 25 Cyberbullying or electronic bullying is where someone, or a group of people, threaten and/or harass someone using social media, instant messaging, email (so called ‘flame mail’) or text messaging. Where employees are subject to such practice they are advised to respond as follows:
 - a if the originator of the material is an employee they should consider resolving the matter through the *Grievance Procedures*. The University reserves the right to investigate and manage any complaints under the *Disciplinary Procedures* where a breach of conduct is alleged.
 - b if the originator of the material is a student they should report this to their 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 they should immediately report this to their manager and/or HR Business Partner.
 - d if the originator of the material has no connection to the University they should consider reporting the matter to the police.
- 26 Additional guidance can be found in the University’s *Dignity at Work Policy*.

General guidance

- 27 Employees should think about their own privacy and check a site’s privacy statement to see what they are signing up to and set privacy settings appropriately. Social network pages, blogs etc. are public. Employees should not put information on them that they do not want others to see. Once information has been posted it can be very difficult to remove. Even if an employee elects to unsubscribe from a site the information may continue to remain visible for a long time.

- 28 Some services will ask individuals to complete a registration form before they can be used. All companies who collect personal information have to state how personal information will be used. This information is contained in the website's terms and conditions.

Monitoring

- 29 The Marketing and Student Recruitment Directorate monitors social media for content relating to the University in order to protect and enhance the reputation of the University and engage with a range of stakeholders.
- 30 All University web activity is logged, and access to sites which are likely to cause a breach of the *Regulations for the use of Computing Facilities* may be blocked. The University reserves the right to sanction investigation and inspection of electronic communications, where there is a complaint or an infringement of the regulations or the rules of the University.

Review

- 31 The policy will be formally reviewed in June 2018 however reviews may take place in the interim to ensure the policy's effectiveness and compliance with legislation, with changes being made accordingly.