Brunel Social Media Use Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security officer

Document History

Version	Author	Comments	Date
V 1.0	Andrew Clarke	First Draft	09/04/2018
V1.1	Andrew Clarke	Amendments for Digital Communications Department responsibilities	11/04/2018
V1.2	Andrew Clarke	Format Changes – Strategy & Governance	03/05/2018
V1.3	Andrew Clarke	Removal of newsgroup reference. Addition of Whistleblowing	18/07/2018
V1.4	Andrew Clarke	Syntax amendments - Head of Infrastructure and Operations	31/07/2018
V1.5	Andrew Clarke	CISA Approval (format changes)	07/09/2018
V1.6	Andrew Clarke	InfoSub Committee – Dr Stephen Swift Comms team authorised exemption. (p8)	12/02/2019
	Andrew Clarke	Annual Review	05/03/2020

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 12 Feb 2019
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 12 Feb 2019
Distribution:	

This document requires the approval from BUL as defined in the ISMS Compliance document.

Contents

1. About this document

1.1 Purpose of Document

The purpose of this policy is to outline the acceptable use of Social Media within Brunel University London. It should be clear that policy is not immutable: in particular, in a field such as this, where emerging technology is interwoven with emerging law, we must be able to react to changes. In the formulation and continuous reformulation of policy, we must be guided by advice from within Brunel University London and beyond, taking due consideration of legal precedent, and having due regard to the practices and experiences of our colleagues in other institutions.

Social networking in both a business and personal environment can have detrimental effects if not used correctly. This document outlines how the use of social networking should be carried out to safeguard the University.

Please refer to Brunel University London ISMS Document *BUL-GLOS-000 - SyOPs Glossary of Terms* for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Cyber & Information Security Manager	Is responsible for maintaining the Brunel Social Media Use Policy and to ensure that the Policy continues best practice and ensuring compliance with legislative and regulatory requirements.
All Users	It is the responsibility of all users of the Brunel University London's IS services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A8 – Asset Management
ISO 27001:2013 Conformance Control	Information Classification Objective A.8.1.3 Acceptable use of assets

1.4 Scope

This policy applies to employees, contractors, consultants, temporaries, other workers, students and affiliates at Brunel University London, including all personnel affiliated with third parties.

This policy applies to all equipment that is owned or leased by Brunel University London and to the use of information, electronic and computing devices and network resources to conduct Brunel University London business or interact with internal networks and university systems, whether owned or leased by Brunel University London, the employee, or a third party. It also extends to information held on behalf of third parties and partners.

This policy also applies when using your own device to store, access or process information on Brunel University London Information Systems.

This policy applies at all times when using Brunel University London information Systems and not just during your normal working hours.

All employees, contractors, consultants, temporaries, other workers, students and affiliates at Brunel University London and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Brunel University London policies and standards, and local laws and regulation.

Examples of social media types/ sites include:

1. Facebook, Google+ and LinkedIn (social networking)
2. Twitter (micro-blogging)
3. Instagram and Snapchat (Photo and video content)
4. YouTube and Flickr (Photo and video content sharing sites
5. Blogs and personal websites
6. Messaging boards
7. Bookmarking websites

This list is not exhaustive as social media is a constantly evolving area and the types of social media available may change over time.

For this Security Standard the aims and objectives are as follows.

- to ensure the use of Social networking on behalf of the University is carried out safely and securely, representing the University in a professional manor
- to ensure that the University's Staff understand that the use of social networking can also have an effect on the organisation they are employed by

- ensure staff understand their responsibilities when using social media and what should, and should not, be electronically written or posted
- highlight potential risks for when staff post on a social networking site
- document University intentions for the use of social media
- ensure the University communicates the implications of using social media inappropriately
- ensure staff know where they can go for further advice

2.0 Social Media Use Policy

2.1 Digital Communication Staff – The University uses social media as part of its Digital Communication Strategy as the Digital Communication Department has authority to speak on behalf of the University.

It is responsible for managing the University official sites which include Facebook Twitter, Instagram, YouTube, Snapchat, Google+ and LinkedIn.

Social media, like other communication tools, is used to improve the public's understanding of the University and its work and engage with the general public.

When using social media sites, the Digital Communication Department will, on behalf of the University, ensure it:

- is respectful towards students, members of the public and University employees
- does not reveal confidential or sensitive information about students, staff or the University
- updates the channels on a regular basis and respond to users posts
- removes any content posted by other users that is considered offensive or derogatory
- adheres to the Brunel Acceptable Use policy and the Brunel Legislative and Regulatory Framework Policy

2.2 Staff – When using University-owned computers, staff are allowed access to Social Media sites and the ability to post on blog sites and micro-blog sites (such as Twitter). When a member of staff identifies they work for the University and/or discusses their work on any social networking site, they must behave professionally and in a way that respects confidentiality and protects students, members of the public, work colleagues and the reputation of the University.

This Policy sets out staff responsibilities when using social media and the legal implications involved. It is not intended to stop members of staff from using social media sites in their own time, but to outline some areas of best practice and illustrate where problems can arise for individual staff members and the University.

All staff have a responsibility to follow the policy.

Social media has blurred the boundary between the private and professional lives of staff and staff that use social media in their personal life should be mindful that inappropriate use could damage their own reputation and that of the University.

When a member of staff identifies their association with the University by, for example, stating they work for Brunel University, discusses their work and/or posting pictures of themselves in a

provided uniform, they are expected to behave professionally and in a way that is consistent with the University values and policies.

Even if a staff member does not directly associate themselves with the University, their link with the organisation can become known through images on the sites of their friends, on the University website or by and internet search using a search engine.

When using any social media channel, staff should follow the principles outlined below:

- Staff may use personal social media sites during their working hours in accordance with the time agreed by their Line Manager
- Use of personal devices to access social media sites should be limited to allocated break times
- If a member of staff discloses that they work for the University or can be identified as an employee through association with other people, they should ensure their profile and related content is consistent with how the University would expect them to present themselves to colleagues and business contacts
- Staff should make it clear that their views are their own, not those of the University when using personal individual Social media and not authorised University Social Media accounts
- As all official social media sites are managed by the Digital Communication Department, no other teams/staff within the University should set up corporate sites without the authorisation of the Digital Communication Department
- Staff should not set up sites that are made to resemble an official site
- If a member of staff associates themselves with the University on their social media site, they are expected to post under their real name to demonstrate openness, honesty and accountability. If an employee posts under a pseudonym and at a later stage these posts are associated with their real name, all previous posts will be admissible in a disciplinary investigation or hearing
- Posts must not contain anything contrary to the University' equality and inclusion policy. Anything containing racist, sexist, homophobic, sexually explicit, threatening, abusive, disrespectful or other unlawful comments must not be published
- Staff should seek permission from colleagues before posting personal details or images that may link them with the University and should not post anything about someone if they

have been asked not to. Staff must always remove information about a colleague if they have been asked to do so

- Staff should be aware of privacy limitations when posting material using social media, and the extent to which information can be in the public domain
- Whatever is posted on a social media site could be in the public domain immediately or, if initially shared with a limited group of followers or friends, could still be copied and shared or published elsewhere
- Staff should carefully consider what they want to say before they publish anything, and work on the basis that anything they write or post could be shared more widely without their knowledge or permission
- Staff should be careful when sharing or retweeting posts, as they could be seen to be endorsing someone else's point of view
- Staff must ensure the information they posts is factually correct. If they discover they have reported something incorrectly, they should amend it and make it clear they have done so
- All comments must be legal and must not incite people to commit a crime
- Staff could face legal proceedings for posted comments aimed at named individuals or an organisation that are considered to harm reputation(s)
- Staff must not use the University logo or University Crest anywhere on their social media sites, or copy photos from the University internet or intranet sites – these are copyright protected
- Staff must not use copyrighted or export controlled materials or any other Brunel University London intellectual property anywhere on their social media sites
- Staff should only share information about the University that is in the public domain, and should not add derogatory comments on these issues
- Staff must also respect student confidentiality, and should not disclose information that could identify a student
- Staff should not air grievances or publish anything that risks bringing the University into disrepute
- If staff post any photos of themselves or colleagues in uniform, or in an identifiable work setting, they must ensure that these represent a professional image of the University. Staff should not use a photo of themselves in uniform as their profile picture this could give the impression that their site is an official site
- Staff must not post images containing students on personal social media accounts. They should also not post images of any incidents they have attended. This does not prevent

staff sharing, retweeting or linking to images that have been published on the official University site
- Staff must not post the same or similar non-business-related messages to large numbers of Social Networking sites (spam)

In addition, staff should configure their privacy settings and review them regularly as:

- Social media sites cannot guarantee confidentiality and are able to change their settings without prior notification
- the public, employers or any organisation staff have a relationship with may be able to access their personal information
- once information is online, it can be difficult to remove it

2.3 Protecting the Whistleblower

The restrictions on the use of Social Media by staff cannot be used to prevent the actions required to disclose any serious concerns that you have about service provision or the conduct of members of the University or others acting on behalf of the University that:

- make you feel uncomfortable in terms of known standards
- are not in keeping with the University's policies
- fall below established standards of practice or
- are improper behaviour.

This caveat has been written to take account of the Public Interest Disclosure Act 1998 which protects workers making disclosures about certain matters of concern, when those disclosures are made in accordance with the Act's provisions and in the public interest.

The Act makes it unlawful for the University to dismiss anyone or allow them to be victimised on the basis that they have made an appropriate lawful disclosure in accordance with the Act.