

Social media and other third-party websites

Compliance Policy

|  |  |  |
| --- | --- | --- |
| **Rev** | **Date** | **Purpose of Issue/Description of Change** |
| 1. | 8 June 2015 | Initial Issue - Version 1 |
| 2. | 16 October 2020 | Review of existing policy |
| 3 | 16 January 2024 | Review of existing policy |
| 4 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy Officer** | **Senior Responsible Officer** | **Approved By** | **Date** |
| Chief Marketing Officer | Head of Communications  | Compliance Committee | 16 January 2024 |

# Scope

This Policy applies to

* all members of staff (those who are managing and/or contributing to corporate social media accounts, those who make contributions to third party accounts where that contribution links to the University either by content or the account that the post is made from, and with regards to their own personal use of social media.
* volunteers or parties acting on behalf of the University.

*This policy should be read in conjunction with the following University Policies.*

* *Privacy Policy*
* *Data Protection Policy*
* *Acceptable Use Regulations*
* *Information Security Policy*
* *Declaration of Interest Policy*
* *Public Interest Disclosure (Whistleblowing) Policy and Procedures*
* *Dignity at Work and Study Policy*

# Definitions

**Staff:** is used in the broader sense and Includes individuals who are undertaking official duties on behalf of the University either in an employed or volunteer capacity (e.g., student wardens, peer guides, interns, open day volunteers, consultants etc.). Although some of the above will not be directly employed by the University, the principles of this policy will apply to them in the same manner.

**Social media:** Websites, platforms and applications that enable users to create and share content or to participate in social networking. Examples of popular social media sites include but are not limited to: LinkedIn; X (formerly Twitter); Facebook; YouTube; TikTok; Instagram; Snapchat; Yammer; Yahoo/MSN messenger; Wikis and blogs; and Weibo.

**Corporate social media account:** Any account run by a College, Department, School, group or other function which sits within the University.

**Third party social media account**: Any account that is not managed by University staff, for example a personal account of the social media account listed above.

# Introduction

Social media channels provide important and exciting opportunities for the University and its constituent parts to communicate and engage with a wide range of audiences and stakeholders. These channels also provide a range of professional and personal opportunities for staff and students.

However, there are several risks associated with the use of social media which could ultimately impact on the University’s reputation.

This policy provides guidance to staff on how to safely use social media and maximise the range of benefits it offers whilst mitigating associated risks. In particular, it provides information on responsibilities when communicating via corporate social media accounts.

The policy also sets out expectations of staff members in the use of individual personal accounts.

Online media is a fast-moving technology, and it is therefore impossible to cover all circumstances. However, the principles set out in this document should always be followed.

The intention of this document is not to stop individuals from conducting legitimate activities using social media but serves to flag up those areas where potential issues may arise.

Any infringement of the Policy will be treated seriously by the University and may be considered a disciplinary matter for those directly employed by the University, and under the relevant policy for those not directly employed.

# Objective(s)

The objective of this policy is:

* To provide staff with information on University requirements and expectations regarding social media;
* To ensure a consistent approach to social media across the institution;
* To set out the legal risks associated with social media use;
* To ensure staff do not compromise their personal security or the security of University information assets;
* To set out the responsibilities of users of corporate social media accounts;
* To support users of corporate social media accounts to mitigate the risks associated with social media, protecting themselves as well as the University;
* To clarify the expectations of staff using social media in an individual professional or personal capacity;
* To outline channels for escalation of issues or concerns;
* To signpost staff to resources which will support them in enhancing their social media presence and that of the University.

# Legal Risks

Staff and students using social media should be mindful of the following legal risks and acts including, but not limited to:

* + - Defamation: posting untrue content adversely affecting a person’s or organisation’s reputation, which has caused, or is likely to cause, harm
		- Malicious falsehood: posting untrue and damaging content with an improper motive, resulting in financial loss for the subject
		- Harassment: subjecting someone to a course of conduct that causes them distress or alarm, including stalking, trolling and cyber-bullying
		- Intellectual property infringement: posting content which copies a substantial part of a work protected by copyright

# Staff responsibilities

#  Overarching requirements:

* **Appropriate use:** In relation to personal use of social media, staff may make reasonable and appropriate use of social media from Bangor University devices. Time spent on social media during working hours should not interfere with other duties.

# Public Interest Disclosure (whistleblowing): Any disclosure of serious malpractice, corruption, wrongdoing or impropriety should be made to the University Secretary. Where an employee releases such information through social media, the University’s [Public Interest](https://www.liverpool.ac.uk/intranet/hr/my-hr/information/policies/) [Disclosure Policy](https://www.liverpool.ac.uk/intranet/hr/my-hr/information/policies/) may be initiated before any further action is taken.

# Dignity at Work and Study: Use of social media should be in accordance with the principles contained with the Dignity at Work and Study Policy, which aims to promote and provide equality, inclusivity, fairness and respect for all in our employment, all who study with us and all who we engage with.

# Corporate Social Media Accounts

There are many live corporate social media accounts for Bangor University. These can be obtained from the Media and Communications team (communications@bangor.ac.uk).

Before creating a corporate social media account, it is important that staff consider whether there is a different audience or set of objectives which cannot be met through an existing account.

An activity plan should be created which considers: the target audience and their information needs; the content to be shared; how producing content and monitoring the account will be resourced; and how this account sits together with those already established across the University.

If a new account is established, the login names must be known to at least two people within a College, School or Department and staff must register the account, password, and name(s) of responsible staff with communications@bangor.ac.uk.

This is important for emergency situations and to ensure colleagues across the institution are kept up to date with policy changes and training opportunities.

Once an account is established, the users need to adhere to this policy and [social media guidelines](https://my.bangor.ac.uk/mrc/documents/Social%20Media%20Guidelines%20March%202022.pdf) which includes details on managing, monitoring and information regarding style.

If a member of staff no longer has responsibility for a social media account, including if they are no longer employed by Bangor University, their respective Line Manager [who? and do we have a process for this?] must arrange to have their access to any University Social Media Accounts removed.

# Corporate Social Media Account Management

**Brand:** All corporate social media accounts must adhere to the University’s brand guidelines. The account profile should clearly state the purpose of the account and the hours during which it is monitored.

To maintain a suite of social presences without any confusion about what is ‘official’ and what is not, staff should consider their avatar, profile, and background images to be extensions of their corporate web presence.

If you do not have a visual aesthetic to your web presence, consider social media your opportunity to give yourself a consistent, recognisable look and feel. The University’s brand guidelines can be found [here](http://www.bangor.ac.uk/ccm/brand/).

When replying to messages and enquiries written in Welsh, either public or private, it is recommended that the reply is in Welsh. All other languages can be replied to in English.

**Language Policy** - All University accounts will provide information in both Welsh and English and will be published in accordance with [Bangor University’s Welsh Language Policy](https://www.bangor.ac.uk/canolfanbedwyr/pdf/Welsh_Language_Policy_revised_2023.pdf). The policy, in compliance with specific Standards placed upon the University, notes that: **‘Corporate and departmental social media accounts will be bilingual and will be active in both Welsh and English.’** \*

Furthermore, this policy adopts the principles that underpin the work of the Welsh Language Commissioner, namely that:

* the Welsh language should be treated no less favourably than English in Wales.
* people in Wales should be able to live their lives through the medium of the Welsh language if they choose to do so.

On social media platforms this can be achieved by either having a fully bilingual account or alternative account for each language. Whichever option is chosen, messages must be posted in both languages simultaneously and to a similar standard in both content and style. However, this does not mean that both versions of a message need to be carbon copies of one another. Staff are encouraged to utilise the University’s bilingual assets and expertise to create content that is creative and suitable for its various audiences.

When replying to messages and enquiries written in Welsh, either public or private, the reply will be in Welsh, in accordance with the Welsh Language Policy.

Further guidance is available from Canolfan Bedwyr, the University’s Centre for Welsh Language Services, Research and Technology: canolfanbedwyr@bangor.ac.uk

\* The only exception to this are those accounts with content aimed specifically at an audience or audiences outside of Wales (for example, an account utilised for the recruitment of students from specific international markets).

# Corporate Social media posts

All posts from corporate social media accounts represent the University.

It is important that messages posted are carefully considered, appropriate and do not damage the reputation of the University or otherwise bring it into disrepute. Safeguards should be put in place to minimise the risk of communication errors via social media, including checking content with a colleague before publishing and where relevant checked with external stakeholders if post relates/mentions a third party.

Those posting content on corporate social media accounts must not:

* post or promote content which harasses, bullies or otherwise intimidates;
* post or promote content which instructs, causes or coerces others to harass, bully or otherwise intimidate;
* post or promote content intended to incite violence or hatred;
* post or promote abusive content relating to an individual’s age, disability, gender reassignment, marriage/civil partnership, pregnancy/maternity, race, religion or belief, sex or sexual orientation.
* include confidential information about an individual or organisation;
* discuss the University’s internal workings or reveal future plans that have not been communicated to the public;
* reveal intellectual property;
* breach the professionalism and confidentiality rules of their area of the University. For example, accounts must not breach confidentiality in clinical cases;
* use someone else’s images or written content without permission and /or without acknowledgement.

# Content principles

Content on all our official social networking pages should be:

* **Varied** – content can include news, events, video, links to campaigns and website updates
* **Frequent** – content should be updated/uploaded at least every other day on Facebook and Twitter and at least weekly on other sites. All pages should be monitored at least twice daily
* **Credible** – although content can be fun it also has to relate to our objectives in terms of raising Bangor’s profile and reputation
* **Clickable** – where possible there should be a link to related content on our official web pages

It is important that content is accurate and does not commit to something which the University does not intend to deliver. If a mistake is made, it is important to be transparent and update the page with a correction.

It is important that all social media accounts are kept up to date, posted from regularly and monitored on a frequent basis. Questions should be responded to promptly within operating hours.

Where several members of staff require access to the same social media account, there must be an agreed overall account manager.

**Accessibility -** All film content which is externally produced or produced in advance for use in a social media campaign must have subtitles for accessibility purposes.

It is accepted that some film content for social media is either livestreamed or produced for immediate use. In such instances, subtitles are not required but a full transcript of audio content of such clips should be made available on request.

# Individuals’ personal and professional accounts

Social media can be an important tool for staff’s professional activity and provide a helpful platform for profile raising and enhancing networks. It is recommended that staff using social media for both professional and personal reasons maintain separate accounts for these purposes as the audiences for each activity are often distinct.

Individuals’ personal and professional accounts should not use Bangor University branding and, if staff do discuss their work on social media, they should make it clear on their profile statement or elsewhere that the views expressed are their own and do not necessarily reflect those of the University.

All employees should consider what they are posting on their individual accounts. The University does not monitor individuals’ accounts. However, if a concern is raised regarding content posted on a staff member’s social media account and the post is considered to be misconduct (as defined in the *University’s Disciplinary Procedure*), the University has the right to request the removal of content. In addition, the matter may be addressed through the University’s Disciplinary Policy. Serious breaches including, but not limited to, harassment or bullying of colleagues and the misuse of confidential information may constitute gross misconduct and may lead to action including dismissal. Staff should also consult the University’s [*Acceptable Use Regulations*](https://www.bangor.ac.uk/itservices/policies/acceptable-regulations.pdf)for other prohibitive actions.

Individuals should be mindful of the information they post / disclose online and ensure that they are carefully considered, appropriate and do not damage the reputation of the University or otherwise bring it into disrepute Where they associate themselves with the University (through providing work details or joining a Bangor University network for example) they should act in a manner which does not bring the University into disrepute or could give rise to a legal claim against the University.

Members of staff should be aware of who can view their profile and act appropriately. This could relate to friends who are also work colleagues, students, prospective students or individuals who have interaction with the University in some capacity.

Staff should consider the possible impact of posting comments relating to their work environment on social networking sites, and the use of a disclaimer in this regard is not enough. Staff should make it clear on their personal accounts that their comments are their own, and not those of Bangor University.

Staff are also advised to maintain professional boundaries on social media and avoid accepting or requesting potential/current students as ‘friends’ particularly as these students may be under the age of 18 which could raise safeguarding concerns. If a friendship request is received, the line manager should be informed and will ensure that the department that handles social media for the team will contact that individual through that particular social media platform by direct message and explain that the staff member is unable to accept their request due to their position at the University. The individual will be invited to follow official University sites relevant to their interests.

# Account security

Social media accounts are at risk of hacking which can cause significant reputational damage and potentially serious misinformation for stakeholders. All accounts should make use of multi factor authentication, and this may be the overall account manager needs to authorise first device connections and periodic approvals. [Size and font here.] There are also considerable resource implications following on from any breach in security such as a compromised social media account.

Where several members of staff require access to the same social media account, there must be an agreed overall account manager. S/he is responsible for choosing strong and secure passwords. The account manager must also ensure passwords are shared and stored securely.

The social media account manager is responsible for maintaining a full log of staff with access to the account’s password and the password must be changed whenever one of those staff members leaves their role.

Where other colleagues or students are granted temporary access to a corporate social media account (e.g., as part of a social media takeover), a secure temporary new account password must be created and then changed back once the takeover is complete.

In cases of emergency, such as hacking, the Communications team may need urgent out of hours access to any corporate social media account. Each social media account manager must as previously stated ensure that the Communications team has their shared passwords.

# Escalating concerns and issues

If a social media account has been hacked or a post from a corporate account attracts negative comments and it is not clear how best to respond, staff should flag this with the Communications team and seek guidance.

Staff should not actively monitor individual staff or student accounts. However, if a staff member notices, or is made aware of, social media activity on a staff or student account that raises welfare concerns or constitutes misconduct, they should email complaints@bangor.ac.uk.

# Social media in an emergency

Social media can be used to provide important information channels for staff, students and wider stakeholders during an emergency situation, and if used, it is vital that the information provided is timely, consistent and accurate.

All communications on social media from the University in an emergency will only be issued via the central University social media accounts. In order to minimise the risk of issuing conflicting and/or incorrect information, it is vital that no other corporate social media accounts are used to post information or updates during a live incident, in such a scenario we recommend that a post should be uploaded directing followers to the corporate account for any information.

# Additional online activity

# Open access online encyclopaedias: In the course of their work staff may find errors in online encyclopaedias. If staff members edit online encyclopaedias at work the source of the correction may be recorded as a University IP address. The correction may therefore look as if it comes from the University itself. Staff should therefore act in a manner that does not bring the University into disrepute and should not post derogatory, defamatory, offensive, or inaccurate comments or do anything that may cause a legal claim to be brought against the University on any online encyclopaedia.

# Blogging: Staff should always adhere to the requirements of the [University’s Data Protection and Information Security](https://www.bangor.ac.uk/governance-and-compliance/dataprotection/index.php.en) policies when considering disclosure of information.

Many bloggers use their personal blogs to discuss their University work and academic study in ways which benefit the University. This Policy is not intended to restrict this, as long as confidential information or information on other individuals is not revealed. However, staff should inform their Head of School / Director of Professional Service if they intend to discuss their University work and / or academic study online. Staff should act in a manner which does not bring the University into disrepute, or is defamatory, or could give rise to a legal claim.

Blogs or websites that do not identify the blogger as a University employee, do not discuss the University, and are purely about personal matters, would normally fall outside this Policy.

Personal blogs and websites should not be used to attack or defame colleagues. Staff members should respect the privacy and the feelings of others and be aware that if they break the law on a blog (for example by posting something defamatory) they will be personally responsible, and although be carried out in a personal capacity, as with all forms of social media, may result in disciplinary action.

# Staff Blogs: Staff who already have a personal blog or website which indicates in any way that they work at the University should discuss any potential conflicts of interest with their Head of School or Director of Professional Service, in accordance with the University’s Policy on Declaration of Interest. Similarly, staff members who wish to start blogging, and wish to say that they work at the University, should discuss any potential conflicts in advance.

If a blog makes it clear that the author works for the University, it should include a visible disclaimer such as “These are personal views and not those of Bangor University”.

Personal blogs and websites should not reveal confidential information about Bangor University. This might include aspects of University policy or details of internal University discussions. If in doubt about what might be confidential, staff members should consult their line manager.

If a staff member thinks something on their blog or website gives rise to concerns about a conflict of interest and in particular concerns about impartiality or confidentiality, this must be discussed with their line manager.

Staff are allowed to update their personal blog and social media accounts from a University computer subject to the University’s Acceptable Use Regulations.

# Compliance and Monitoring

All members of the University are directly responsible and liable for the information they handle. Staff and students are bound to abide by the University’s Acceptable Use Regulations.

Any misuse or any use that may bring the University into disrepute must be reported to the Head of Legal Service, Legal and Compliance department, in the first instance, and, in consultation with Human Resources, disciplinary action may be taken.

# Review

The policy will be reviewed every three years, or at earlier intervals in light of any changes to legislation, technology or the operation of the existing policy.

# Equality Impact Assessment

This Policy has been Equality Impact Assessed based on the information available at the time of the policy being developed. A further Equality Impact Assessment will be carried out in conjunction with any review of the Policy.