BRIDGWATER & TAUNTON COLLEGE

STAFF SOCIAL MEDIA POLICY

Author:	Digital Marketing Manager
Approved by:	SMT
Date:	May 2019
Review date:	May 2022

CONTENTS

1. Introduction

Bridgwater & Taunton College recognises and embraces the benefits and opportunities that social media can bring as a tool.

For the purposes of this policy, social media is defined as a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes online social forums, anonymous apps, blogs, video-and image-sharing websites and similar facilities.

It can be used to share news, information and successes, keep staff and students up to date with important developments and promote healthy academic debate about controversial subjects and areas of research. Examples include Facebook, Linkedin, YouTube, Instagram, Twitter, Flickr and Pinterest.

There is, however, an inherent risk involved in using social media, in that, it is an instantaneous and far reaching form of communication and inappropriate use can impact upon staff, students and the reputation of the College.

The College encourages employees to engage, collaborate and innovate through social media; however, wherever and whenever the employee does this, they must be aware of the potential impact on both themselves and the College.

Except where otherwise stated, this policy does not form part of any contract of employment and we may amend it at any time.

2. Policy Statement

This policy is intended to minimise the risks of social media which can impact on the wellbeing of students and staff and the reputation of Bridgwater & Taunton College, so that students and staff can enjoy the benefits of social networking whilst understanding the standards of conduct expected by the College.

This policy outlines the standards we require our staff to observe when using social media, the fact that we monitor usage of social media and the action we will take if this policy is breached.

3. Scope

This policy relates to all College employees who create or contribute to blogs, wikis, social networks, apps, forums, virtual worlds, or any other kind of social media. It should be applied to all use and all forms of social media where there is potential impact on the College, whether for work-related or personal use, whether during working hours or otherwise, whether social media is accessed using the College's IT facilities and equipment, or equipment belongs to members of staff or any other third party.

4. Legislation

There are a number of pieces of legislation relevant to the use of social media and these are listed in Appendix A. Staff using social media should be mindful of the following legal risks and acts in particular.

- 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.
- Breach of confidence: posting confidential information.
- Malicious Communications Act 1988: prevents conveying a threat, a grossly offensive or indecent message or false information with the intention to cause distress or anxiety to the reader or recipient.
- Section 127, Communications Act 2003: prevents the use of public electronic communications equipment to send a message that is false, grossly offensive, or of an indecent, obscene or menacing character, whether received by the intended recipient or not.
- Computer Misuse Act 1990: prevents the unauthorised access, modification and use of computer material or the use of a computer to assist in a criminal offence, including accessing confidential information and thereby impersonating another person through social media.
- Prevent Duty Guidance (from Section 26(1) of the Counter-Terrorism and Security Act 2015): requires the College to have due regard to the need to prevent people from being drawn into terrorism.
- The Public Sector Equality Duty (Section 146 of the Equality Act 2010): requires the College to have due regard to the need to eliminate unlawful discrimination, including bullying, harassment and victimisation; to promote equality of opportunity between different groups; and to foster good relations between different groups.

5. Monitoring

Our IT Acceptable Use Policy sets out the College's right to monitor, intercept and read communications, and applies equally to the use of social media platforms.

The College will also monitor how the College uses social media generally and what is said about it and about other colleges. The Head of IT Services is responsible for this monitoring.

6. Acceptable Use of Social Media at Work

The College IT systems are first and foremost a business tool and using these for personal reasons is a privilege not a right, and is subject to the restrictions set out in this policy. Staff contributing to the College's social media activities should remember that they are representing the College. The following rules should be followed:

- Staff should only comment within their own area of expertise to provide individual perspectives on non-confidential activities at the College.
- Employees should never represent themselves or Bridgwater & Taunton College in a false or misleading way. All statements must be true and not misleading; all claims must be substantiated.
- Use common sense and common courtesy: staff should ask permission to publish or report conversations that are meant to be private or internal to the College.
- Where employees access social media for work-related purposes or personal use using the College's IT facilities and equipment, the College's e-safety Policy will apply.
- Employees should seek guidance before participating in social media when the topic being discussed may be considered sensitive (e.g. a crisis situation, intellectual property, issues which may impact on the College's reputation, commercially sensitive material). Social

media activity around sensitive topics should be referred to the Director of Business Development & Marketing

- If an employee's use of social media is considered to be derogatory, discriminatory, bullying, threatening, defamatory, offensive, intimidating, harassing, creating legal liability for the College, bringing the College into disrepute, breaching College policies and procedures, such as the Dignity at Work policy or causes Safeguarding/Child Protection concerns, then the College may take action under the staff disciplinary procedure. This may include comments, videos, or photographs, which have been posted on social media sites about the College, students, work colleagues or managers.
- An employee should not engage in illegal activity through social media or engage in any activity that promotes terrorism. The very fact of possessing or disseminating terrorist material may be sufficient to warrant an investigation by the police and a member of staff would be put in the position of having to advance a credible defence.
- The College's response to any misuse of social media in a personal capacity will be reasonable and proportionate to the perceived offence; the nature of the postings/comments made and the impact or potential impact on the College, its staff, stakeholders and/or students.
- Social networking sites may be referred to when investigating possible misconduct/gross misconduct.
- Staff should be aware of security threats and be on guard for social engineering and phishing attempts. Social networks can also be used to distribute spam and malware.
- Bridgwater & Taunton College may require employees to remove social media postings which are deemed to constitute a breach of these standards and failure to comply with such a request may, in itself, result in disciplinary action.
- The College accepts that employees may wish to use social media as a way of communicating personally, however its use at work should be restricted to the terms of this policy. Employees are permitted to make reasonable and appropriate use of social media websites from the College IT system during official breaks.
- The use of personal devices to access social media websites at work should be limited to official breaks and not when expected to be carrying out their work duties.

7. Responsibilities

- Employees should be transparent and state that they work for Bridgwater & Taunton College if they are posting about the College. If you are writing about the College or a competitor, use your real name, identify that you work for the College, and be clear about your role. The College discourages staff from posting online anonymously or using pseudonyms. You should never impersonate another individual.
- Employees should not provide references or recommendations for anyone else on social media (whether employment or business recommendations) in any way that suggests any endorsement or recommendation by the College; in such cases as disclaimer stating "The views expressed are my own and do not necessarily reflect the views of the College".
- Ensure that all communications are of high quality (in terms of content and form) including being grammatically correct, accurate, objectively justifiable, reasonable and appropriate for the intended audience.
- Line managers are responsible for addressing any concerns and/or questions arising out of the use of social media, and should refer to HR where the concerns may lead to disciplinary action.
- Employees are responsible for their words and actions in an online environment and are therefore advised to consider whether any comment, photograph or video they are about to post on a social networking site, is something that they would want students, colleagues and other employees of the College, their manager or people outside the College to read.
- Marketing are responsible for giving specialist advice on the use of social media for College business, and if employees become aware of any adverse criticism of the College

should inform the Head of Marketing/Digital Marketing Manager – staff should not respond without express approval.

8. Expected Standards of Conduct on Social Media Websites

Appropriate Conduct

Staff may not use their work email address to sign up for personal social media websites.

Staff should have no expectation of privacy or confidentiality in anything created or shared on social media platforms. When creating or exchanging content using social you are making a public statement and as such will not be private and can be forwarded to third parties without your consent. Employees are therefore encouraged to consider the sensitivity of disclosing information to the world. Once sensitive or confidential information (or offensive or defamatory information) has been disclosed, it cannot be recovered and this may result in liability both for the College and also you personally.

Employees should also be aware that even when using social media in a personal capacity, other users may be aware of their association with the College and may reasonably think they are speaking on the College's behalf. Employees should also consider any adverse impact content posted on social media may have on the College's reputation or supplier relationships.

When creating or exchanging content on a social media platform, staff must comply with the terms of the contract of employment, the Disciplinary Policy and any other policies that may be relevant. In particular staff must:

- Not harass or bully other members of staff or breach the College's Dignity At Work Policy.
- Not discriminate against any members of staff, students or third party or breach the College's Equality & Diversity Policy.
- Not break the College's Data Protection, IT Acceptable Use, Use of Email and Whistleblowing Policies
- Respect confidentiality obligations owed by members of staff or the College, and not disclose commercially sensitive material or infringe any intellectual property or privacy rights of the College or any third party.
- Not make defamatory or disparaging statements about the College, its staff or students or other colleges.
- Not create or exchange or link to abusive, obscene, discriminatory, derogatory, defamatory or pornographic content:
- Not upload, post or forward any content belonging to a third party unless you have that third party's consent.
- Ensure that any quotes from third party material are accurate.
- Check that a third party website permits you to link to it before including a lnk and ensure that the link makes clear to the user that the link will take them to the third party's site and not post, upload, forward or post a link to chain mail, junk mail, cartoons, jokes or gossip.
- Do not escalate "heated" discussions, and do not discuss topics that may be inflammatory, such as politics or religion.
- Regularly review privacy settings on personal social media accounts and review the content of your personal social media accounts and delete anything that could reflect negatively in a professional capacity or on the College.

Acceptance of Friends

Employees **must not** accept and/or invite the following individuals to be "friends" on personal social media accounts, closed groups or other online services:

- Students of any age
- Ex-students under the age of 18
- Parents/guardians/carers/wards of students under the age of 18

Entering into such relationships may lead to abuse or accusations of abuse of an employee's position of trust and breach of standards of professional behaviour and conduct expected by the College. The College reserves the right to take disciplinary actions if employees are found to be in breach of this policy, with the potential of dismissal for serious breaches.

Acts of a criminal nature or any safeguarding concerns must be referred to designated safeguarding leads and/or the Principal, who may report the matter to the police, Local Safeguarding Children Board (LSCB) and or the Independent Safeguarding Authority (ISA) if appropriate.

If an employee is "friends" on personal social media accounts or other online services with students of any age, ex-students under the age of 18 and/or parents due to a justified reason (for example, the person is a family member), this must be declared to your line manager.

9. Use of Social Media during Recruitment & Selection Process

The College may view relevant social media websites as part of the pre-employment process. Where this is done the College will act in accordance with the data protection and equality & diversity obligations.

10. Inappropriate Conduct and Excessive Use

If an employee is found to be in breach of this policy they will be disciplined in accordance with our Disciplinary Policy. In certain circumstances breach of this policy may be considered gross misconduct which may lead to immediate dismissal without notice. Alternatively, the College may choose to withdraw access to social media platforms for that individual. Employees should note, in particular, that creating

Employees should be aware that creating or sharing content on a social media platform may amount to misconduct even if it takes place:

- On a personal account with appropriate privacy settings
- Outside normal working hours; and/or
- Without using our computers, systems or networks.

The College will use the Disciplinary Policy to address issues of excessive use of social media platforms during working hours.

11. Social Media Account Management

All corporate social media accounts must adhere to the College's brand guidelines and the account profile information should clearly state the purpose of the account and the hours during which it is monitored.

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.

All social media accounts and account managers must be logged with the College's Marketing team.

12. Other relevant policies and documents

This policy should not be read in isolation but should be cross-referenced to other relevant College employment and student policies and procedures, including:

- Online Safety Policy
- Safeguarding and Child Protection Policy and Procedure
- IT Acceptable Use Policy
- Mobile Device Policy and Procedure
- Staff Disciplinary Policy and Procedures
- Data Protection Policy and Procedure
- Keeping Children Safe in Education Part 1 (2018)

13. Review of policy

This policy will be reviewed in line with legislative changes, case law or no later than 3 years after the issue date.

Appendix A - Legislation

Relevant legislation includes:

- Communications Act 2003
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Counter Terrorism and Security Act 2015 (Prevent)
- Criminal Justice and Immigration Act 2008
- Data Protection Act 1998
- Data Retention Investigatory Powers Act 2014
- Defamation Act 2013
- Education (No. 2) Act 1986 (Freedom of Speech)
- Education Act 1986; Education Reform Act 1988 (Academic Freedom)
- Employment Rights Act 1996
- Equality Act 2010
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002
- Human Rights Act 1998
- Malicious Communications Act 1988
- Obscene Publications Act 1959 and 1964
- Police and Criminal Evidence Act 1984
- Police and Justice Act 2006
- Prevention of Terrorism Act 2005
- Protection from Harassment Act 1997
- Protection of Children Act 1978
- Public Order Act 1986 (as amended by the Racial and Religious Hatred Act 2007)
- Regulation of Investigatory Powers Act 2000
- Terrorism Act 2006