GENERAL POLICY: SOCIAL MEDIA

Applies to both staff and learners

This policy is biennially reviewed to ensure compliance with current regulations

Approved/reviewed by	
Executive Director: People	
Date of next review	**February 2024**

This policy and procedure is subject to The Equality Act 2010 which recognises the following categories of individual as Protected Characteristics: Age, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex (gender), Sexual orientation, Disability, Socio-Economic Disadvantage

1. Document Control

1.1. Document Details

Title	Social Media Policy
Author	Dawn Telford / Jen Durrant
Version	2.0
Date	Feb 2022
Status	Published

1.2. Revision History

Version	Date	Author	Comments
1.0	Feb 20	Dawn Telford / Jen Durrant	Definitive Release
2.0	Feb 22	Dawn Telford / Jen Durrant	Definitive Release

1.3. Distribution

Name	Email	Organisation
All Staff	SharePoint upload	Boston College

1. INTRODUCTION

This policy outlines the responsibilities of employees when accessing social media either personally or using it for College purposes. It aims to manage organisational risks when social media is used for both business and personal use, and to ensure that its use is acceptable to avoid bringing the College into disrepute. This guidance supports the College policy named Email and Internet.

For the purposes of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other or share data in the public domain. This includes but is not restricted to online social forums such as Twitter, Facebook, WordPress, Myspace, Instagram and Linkedin. Social media also covers blogs and video-and image-sharing websites such as YouTube and Flickr.

Employers should be aware that there are many more examples of social media as it is a constantly changing area. Employees should follow these guidelines in relation to any social media that they use.

The College recognises the value that social media can have to our business if used in a responsible and professional way. While it is recognised that employees are entitled to a private life, the College is committed to maintaining confidentiality and professionalism at all times whilst also upholding its reputation by ensuring employees exhibit acceptable behaviours.

2. SCOPE

This policy applies to all employees employed by the College. Our commitment to equality of opportunity also extends to applicants who apply to work in the College.

Although this policy refers to employees throughout, the College is aware of its wider responsibilities to provide a positive working environment for all who work on the College premises.

Individuals are personally accountable for their behaviour and may be held liable for any breaches of this policy. All individuals who work on college premises, including agency, contract workers and volunteers are therefore expected to support the College's policy on social media.

Staff should remind learners of their responsibilities and the risks in relation to the use of social media in line with the Education Inspection Framework and the Prevent Duty.

3. LEGISLATION

The College will adhere to its obligations under the legislation relevant to the use and monitoring of electronic communications, which are predominately the Regulation of Investigatory Powers Act 2000; the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000; the

Communications Act 2003; Data Protection Act 1998; the Human Rights Act 1998; the Defamation Act 1996 and the Equality Act 2010.

Section 26 (1) of the Counter Terrorism and Security Act 2015 imposes a duty on the College, when exercising their functions, to have due regard for the need to prevent individuals from being drawn into terrorism. This does not include just violent extremism but also non-violent extremism, which can create an atmosphere conducive to terrorism and can popularise views which terrorists exploit.

4. DATA PROTECTION AND MONITORING

Computers are the property of the College and are primarily designed to assist in the performance of work duties or study. To ensure appropriate use of the internet, the College's internet software monitors websites visited by employees and learners for business and security purposes. Therefore, employees should have no expectation of privacy when it comes to the sites they access from College computers and devices.

The College may exercise its rights to intercept internet access under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 for the following business reasons;

- To establish the existence of facts relevant to the College's business.
- To ascertain compliance with regulatory practices or procedures relevant to the College.
- To ensure that employees using the system are achieving the standards required.
- To prevent or detect crime.
- To investigate or detect the unauthorised use or abuse of the telecommunications systems, including using inappropriate use of social media websites.
- To ensure effective operation of systems, e.g. to detect computer viruses and to maintain an adequate level of security.

5. PRIVACY SETTINGS AND PERSONAL INFORMATION

Default privacy settings for some social media websites allow some information to be shared beyond an individual's contacts. In such situations, the user of the site is personally responsible for adjusting the privacy settings for the account. Information available on social media sites could be produced as evidence by either a College or employee, should it be necessary either as part of College procedures, or in legal proceedings.

Therefore, it is vital that employees and learners are strongly encouraged to review their access and privacy settings for any social media sites to control, restrict and guard against who can access the information on those sites. Even if privacy and

security settings are utilised, anything posted on social media sites may be made public by onward transmission.

To avoid identity theft, employees and learners are advised to refrain from publishing any personal or sensitive information on social media websites, e.g. date of birth, home address, telephone number or any information related to personal bank accounts.

6. ACCEPTABLE USE OF SOCIAL MEDIA AT WORK

The College IT Systems are first and foremost business tools, and as such personal usage of the systems is a privilege and not a right. Employees are permitted to make reasonable and appropriate use of social media websites where this is part of the normal duties of their work for example Marketing staff. The College has blocked the use of certain social media websites such as Facebook, Bebo and 'My space' from the College's computers. Therefore staff and learners are not allowed to access such social media websites without being granted permission from the Quality team and IT department.

Staff responsible for contributing to the College's social media activities should be aware at all times that they are representing the College. Employees who use social media as part of their job should adhere to the following rules: -

- All staff are expected to liaise with Marketing to use the College Facebook site to promote events and news at the College.

- For Curriculum staff who want to use a social media site to promote their area, personal accounts must NOT be used and approval should be sought from the Quality team before setting up a generic account that they wish learners to access.

- Once approval has been granted and before allowing learners to access the Facebook page, academic staff should remind learners of their responsibilities in relation to social media.

- Curriculum staff should read the social media guidance notes and be aware of their own responsibilities, which includes the role of monitoring before placing any course material on a social media site.

- Employees may wish to use their own personal devices, (including laptops, palm-tops, hand-held devices and smart phones) to access social media websites, whilst at work, but this should be restricted to their rest breaks.

- Personal use of social media is not acceptable during working hours except in authorised breaks. If the College views the personal use to be excessive then this will be considered a disciplinary offence.

7.1 APPROPIATE CONDUCT

The line between public and private, professional and personal is not always clearly defined when using social media. If an employee or learner identifies themselves as

a part of the College, this has the potential to create perceptions about the College to a range of external audiences and also among colleagues and learners.

When communicating either in a professional or personal capacity, within or outside the workplace, employees **must**: -

- Conduct themselves in accordance with other policies, procedures and the (College code of professional conduct) particularly when using College social media accounts to portray the College's activities, as this is an extension of the College's infrastructure.

- Be professional, courteous and respectful as would be expected in any other situation.

- Think carefully about how and what activities are carried out on social media websites.

- Be transparent and honest. The College will not tolerate employees making false representations. If employees express personal views, it should be made clear that the views do not represent or reflect the views of the College.

- Remove or request the removal of any inappropriate comments, images or videos of them

7.2 INAPPROPRIATE CONDUCT

While using social media in any capacity, employees' or learners actions can still damage the College's reputation.

When communicating either in a professional or personal capacity, within or outside the workplace, employees or learners **must not** conduct themselves inappropriately. The following are examples of inappropriate conduct: -

- Engaging in activities that have the potential to bring the College into disrepute.

- Breach of confidentiality by disclosing privileged, sensitive and/or confidential information.

  Making comments that could be considered to be bullying, harassing or discriminatory against any individual. For example making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age.

- Posting remarks which may inadvertently cause offence and constitute unlawful discrimination, harassment and / or victimisation.

- Taking pictures of staff, learners or visitors without their explicit consent or consent of parents of the learner is under 18 year of age.

- Posting or uploading inappropriate comments, images, photographs and / or video clips about colleagues or ex-colleagues, learners or ex- learners, parents or clients. This also covers links to such inappropriate content.

- Breach copyright, for example taking or using someone else's images or written content without permission:' or failing to give acknowledgement where permission has been given to reproduce something.

- Publishing defamatory and / or knowingly false material about the College, other employees or learners.

- Engaging in discussions or anything which may contravene the College's Equality and Diversity policy and may have the potential to cause serious harm to the business.

- Blurring the boundaries of professional and personal life, leading to a conflict of interest.

- Pursuing personal relationships with learners, ex-learners or parents.

- Participating in any activity which may compromise your position at the College.

- Behaviour that would not be acceptable in any other situation.

- Knowingly accessing, viewing or downloading material which could cause offence to other people or may be illegal.

- Commenting on any work-related matters.

- Using a College email account to create a personal social media account.

- Using social media websites in any way which is deemed to be unlawful.

- Accessing someone else's social media website page and posting or sending comments in their name.

- Accessing extremist religious or political social media or websites.

The above examples are not exhaustive or exclusive.

Employees will be held personally liable for any material published on social media websites that compromise themselves, their colleagues and / or the College.

7.3 <u>ACCEPTANCE OF FRIENDS</u>

The College encourages the positive use of social media as part of the educational process. Social media is used by many people, particularly learners to communicate with their peers and the public. Learners may wish to form personal relationships with employees, however to ensure professional boundaries are

maintained, employees **must not** accept and / or invite the following individuals to be 'friends' on personal social media accounts or other online services: -

- learners, including vulnerable students who are adults or children,
- ex-learners under the age of 18, and
- parents, guardians or carers of current learners.

Pursuing or entering into such relationships may lead to abuse of an employee's position of trust and breach the standards of professional behaviour and conduct expected at the College. The College reserves the right to take disciplinary action 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 may be referred to the police, Local Safeguarding Children Board (LSCB) and / or the Disclosure and Barring Service (DBS).

If a learner at the College is considered a family friend, please log this with your line manager.

8. USE OF SOCIAL MEDIA DURING RECRUITMENT AND SELECTION PROCESS

The College will only view relevant social media websites as part of the pre-employment process, i.e. those aimed specifically at the professional market and used for networking and career development (e.g. LinkedIn). Any information that relates to applicants' protected characteristics under the Equality Act 2010 will not be used as part of the recruitment and selection process.

Human Resources may liaise with Marketing to advertise vacant posts using the College social media sites.

9. INAPPROPRIATE CONDUCT AND EXCESSIVE USE

All staff are required to adhere to this policy. Any breach of this policy, including inappropriate conduct of the kind listed in section 7 above, or of a similar nature, and any excessive personal use of social media websites will be dealt with in accordance with the College disciplinary procedure.

Disciplinary action may be taken against employees in line with the College disciplinary policy and may also result in (the withdrawal of access to social media websites / withdrawal of internet access). Persistent breaches of this policy may lead to dismissal. Serious breaches may constitute gross misconduct, which may result in summary dismissal.

10. RESPONSIBILITIES

All employees are responsible for complying with the requirements of this policy and for reporting any breaches of the policy to their line manager. However, if the concern

is relating to a safeguarding issue, any staff or volunteers that have such concerns about either a learner, member of staff or volunteer, should refer directly to Safeguarding Team as per the Safeguarding Policy.

If employees have concerns about information or conduct on social media sites that are inappropriate, offensive, demeaning or could be seen to be bullying, this should be reported to their line manager.