Social Media Policy for Staff & Students

Title:	Social Media Policy for Staff & Students	
Document owner:	Julie Sokald – Head of Marketing	
Reviewed/updated by:	Julie Sokald – Head of Marketing	
Version:	1	
Review cycle:	Annual	
Date of update:	April 2026	
Next due:	April 2027	
Approval Level:	SLT	Y by Deputy Principal & CEO
	Governors	N
Date Approved:	June 2026	
Publication:	Intranet	Y
	Website	N
	Students	Y

Version	Author	Date	Section	Changes summary
1	Julie Sokald	April 2026		Whole policy rewritten to bring policy in line with advances in social media use and increase in social media platforms

Social Media Policy for Staff & Students

1. Introduction / purpose of policy

This policy sets out the College's expectations for the responsible, safe and professional use of social media by staff and students. It aims to protect individuals and the College's reputation, while supporting positive and appropriate online engagement.

The policy outlines the standards of conduct expected when using social media, whether on behalf of the College or in a personal capacity where the College may be identified. It also clarifies roles and responsibilities, and the potential consequences of misuse.

This policy applies to all staff and students of the College and should be read alongside other relevant College policies, including safeguarding, behaviour, equality and disciplinary procedures.

2. Scope

This policy applies to all College staff and students at every College campus at Skipton, Ripon and Leeds Bradford Airport, as well as at all community outreach and off-site delivery locations. It also applies to agency workers, contractors, volunteers and any other individuals engaged to work with or on behalf of the College. All those covered by this policy are expected to adhere to its requirements when using social media in connection with the College.

3. Roles and Responsibilities

All staff are responsible for:

- reading and taking the time to ensure that they understand this policy;
- ensuring that any use of social media (professionally and personally) is carried out in line with this and other relevant policies, including the IT Acceptable Use Policy;
- completing any relevant training as required;
- reporting any incidents or concerns regarding social media use to the Marketing Department and Senior Leadership Team

All Head of Department/managers are responsible for:

- reporting and escalating any incidents or concerns regarding social media as appropriate;
- departmental-led social media accounts and all content posted on these accounts
- completing relevant training as required, as well as ensuring their staff are appropriately trained where required
- addressing any issues of misuse of social media by those staff for whom they are responsible.

All college-branded social media account owners are responsible for:

- completing any relevant training as required;
- operating accounts appropriately, and in accordance with this policy and relevant guidelines
- putting in place appropriate security on accounts including password management
- ensuring that accounts have up to date content
- responding to comments
- closing down unused accounts.

4. Acceptable Use of Social Media at College

- Social media for **personal use** is permitted only during **breaks and outside of lessons or work duties**.
- **Educational or professional use** of social media must be approved by a tutor (in the case of students) or manager (in the case of staff).
- Social media access must not interfere with learning, teaching, or operational responsibilities.
- College networks must not be used to access or share inappropriate or unlawful content.
- Misinformation and Disinformation - All staff and students must take care to verify the accuracy of information before posting, sharing, or commenting on social media or online platforms. Sharing false or misleading information, even unintentionally, can damage reputations and the College's public trust.
- The creation or distribution of deepfake or otherwise altered media (audio, image, or video) that misrepresents individuals, the College, or events is strictly prohibited.

5. Standards of Conduct

- Communicate respectfully and professionally online.
- Do not post or endorse discriminatory, defamatory, abusive, or offensive content.
- Refrain from commenting on College matters in a way that could bring the institution into disrepute.
- Students and staff must not engage in cyberbullying or harassment.
- Staff must maintain appropriate boundaries with students, parents and carers and not "friend/connect" or follow students/parent/carer on personal social media accounts (other than in circumstances where the member of staff has a pre-existing personal relationship with that person, which has been declared to their line manager/HR).
- Staff who encourage students to use professional networks such as LinkedIn to support their future careers or further study must provide clear guidance to students on safe and effective use for professional development and networking.
- Staff using LinkedIn should use their own judgement whether they accept connections with Higher Education students above 18 years-old in a strictly professional capacity.

6. Data Protection

- Personal and confidential College information must not be shared online.
- Do not post, share or repost content involving students or staff without their explicit consent. Content published through official College channels will have obtained the appropriate written consent; therefore, resharing directly from official College platforms is permitted.
- Respect secure handling of data in line with the College's Data Protection Policy.

7. Use of Images, Media, Music & Sensitive Content

- Image/video consent must be obtained in writing from students and staff on the College's Image consent form held centrally in Marketing.

- Photos or videos of students, staff, or College facilities must **not be shared externally** without written consent of those involved.
- Recording in classrooms or College spaces requires prior permission.
- Staff must not use their own devices to capture student images or content. To collect this information a college-owned device must be used.
- Staff must follow marketing and safeguarding protocols when using images in College communications.
- Staff and students may reshare College-related content from peers' personal accounts, including images/videos, without prior written approval, provided the content presents the College in a positive and professional light and complies with this policy.
- Staff and students must ensure that any music used in social media content is lawful and does not infringe copyright. Copyrighted music must not be used without the appropriate permissions or licences, and users should only use royalty-free music or audio made available for use within the relevant platform's licensing terms.
- Posts/media that include potentially sensitive content such as realistic fake injuries, dissections of dead animals (for educational purposes), swearing or other graphic imagery, should include a clear *content warning* at the beginning of the post or before any attached media. Example: "Content Warning (or CW): fake blood and special effects makeup used as part of class" or "Contains adult language"

8. Social Media and Staff Recruitment (Staff Only)

- The College may use professional social media platforms (e.g. LinkedIn) as part of the recruitment and selection process. Any information that relates to applicants' protected characteristics under the Equality Act 2010 will not be used as part of the process

9. Privacy Settings and Personal Information (Staff Only)

- Staff are responsible for managing their own privacy settings on social media platforms.
- Content shared, even with privacy settings enabled, can still be shared beyond intended audiences and may be used in College or legal proceedings.
- Staff should not post sensitive personal information (e.g. date of birth, address, bank details) to reduce the risk of identity theft.
- Always follow the College's Acceptable Use Policy when handling passwords and personal data online
- Where staff permit students to access or contribute to College-owned social media accounts, the member of staff remains fully responsible for the security, management and appropriate use of those accounts, including ensuring that passwords and access details are kept secure.

10. Departmental Social Media Accounts (Staff Only)

- Any new departmental or course-specific social media accounts must receive approval from the Marketing Department before being created or launched. The Marketing Department must have admin access to all departmental accounts to ensure safeguarding, branding consistency, and

strategic alignment.

- Accounts created without approval may be subject to closure or integration under College-managed platforms.
- If AI is used, staff must use AI tools on social media responsibly and professionally, ensuring any AI-generated content shared on behalf of the College is accurate, clearly identified as such, and upholds the College's values and safeguarding standards.

Where departments manage their own social media channels, they must adhere to the following:

- **Branding & Tone**: All content must be aligned with the College's official brand, tone, and communication style. Refer to the College Marketing Department for brand guidelines.
- **Grammar & Professionalism**: Posts and content should be clear, grammatically correct, and uphold a professional standard.
- **Relevance & Strategy**: Content should support departmental objectives and the College's overall marketing strategy. Avoid off-topic or personal content.
- **Consent for Images**: Ensure written consent is obtained before posting any images or videos featuring students, staff, or third parties.
- **Security & Access**: Login credentials for departmental accounts must be kept secure and only shared with authorised staff.
- **Oversight**: Departments are responsible for regularly monitoring their accounts. Inactive accounts should be reviewed with the Marketing Department.
- **Crisis Escalation**: Any negative or inappropriate engagement on departmental channels must be reported to the Senior Leadership Team, Marketing and Safeguarding Teams promptly.

11. Student-Generated Content (Projects, Portfolios, or Promotions)

Where students are producing content (e.g. videos, blogs, reels, or photography) that represents or refers to the College:

- All content must comply with this policy and College-wide standards on conduct, privacy, and safeguarding.
- Content must not be created, published, or shared externally without prior approval from both the Marketing Department and the relevant tutor or course lead.
- Students must not use the College logo, branding, or identifiable premises in media without permission from the Marketing department.
- Where students are granted access to College-owned social media accounts, they are responsible for using the account appropriately, maintaining the confidentiality of passwords and access details, and following all College guidelines for security and acceptable use.
- Students must not use AI tools on social media to create or share misleading, offensive, or deceptive content (including deepfakes), and should clearly indicate when AI has been used to generate material they post or share.
- Any students appearing in content must have provided signed, informed consent.

- The College reserves the right to request the removal or editing of student content that misrepresents the College or violates College policies.

12. Reporting Harmful or Inappropriate Content

- Any harmful, inappropriate or concerning social media content relating to the College must be reported immediately. Staff and students should contact the Marketing Department in the first instance or inform their Head of Department or Senior Leadership Team without delay**.**

Non-compliance with this policy may lead to disciplinary action in accordance with the College's Disciplinary Policies. In serious cases, breaches may also be referred to external authorities.

13. Legislation and Regulatory Compliance

- Education Act 2002
- Keeping Children Safe in Education (KCSIE) Keeping children safe in education - GOV.UK
- Equality Act 2010
- The Copyright Designs and Patents Act (1988)
- UK General Data Protection Regulation (UK GDPR)
- Generative AI:Product Safety Expectations
- Prevent Duty Guidance FE/HE (2023)
- UK Council for Internet Safety

14. Monitoring and Review

This policy will be reviewed annually by the Head of Marketing and will be approved by the Senior Leadership Team.

15. Related Policies and Documents

- ICT Acceptable Use Policy
- Staff Code of Conduct
- Student Code of Conduct
- Student Positive Behaviour Policy
- Safeguarding Policy and Safeguarding Children and Vulnerable Adults
- Data Protection Policy
- Disciplinary and Dismissal Procedures
- Grievance Procedure
- Whistleblowing Policy
- Bullying and Harassment Policy
- Equality & Diversity Policy
- Health and Safety Policy
- Zero Tolerance Policy
- Craven College Brand Guidelines