MORLEY COLLEGE LONDON

Social Media Policy
For Staff

POLICY OWNER:	Head of Marketing and Sales
FINAL APPROVAL BY:	Policy Committee
Policy Category:	Corporate
Approved by Policy Committee:	November 2023
Approved by Governing Body:	N/A
Review Date:	November 2027
Last Updated:	*April 2024*

1. Introduction, Purpose and Scope of Policy:

1.1 Morley College London is committed to becoming a leading London college where learning excites ambition and enables achievement. The College recognises the evolving benefits of social media in achieving this vision and encourages staff to use it as a tool for communication, collaboration and community building.

1.2 This policy is designed to provide clear guidelines for the appropriate, safe and effective use of social media platforms, whilst raising awareness of the potential impacts on the College and individuals.

2. Equality and Diversity Analysis Screening:

2.1 In accordance with the Morley's Equality, Diversity and Inclusion Statement the development of this policy complies with the Equality Act 2010 in ensuring due regard to eliminating discrimination, advancing equality of opportunity and fostering good relations.

2.2 An impact analysis was not required for this policy as it has no bearing on the general equality duty.

3. Applicability:

3.1 This policy applies to all Morley College London staff, contractors and volunteers, including governors, who may use social media in both professional or personal capacities to communicate:

- Content that identifies them as a Morley College London staff member, contractor or volunteer, including governor,
- Content relating to others within the Morley,
- Content created in connection with their Morley employment,
- Content about Morley College London.

3.2 This policy applies to the use of all forms of social media used to communicate content that may impact Morley, regardless of:

- whether for work or personal related purposes;
- whether during work hours or not;
- whether accessed from the College premises or offsite;
- whether accessed via the College's IT facilities and issued-devices, personal devices or those belonging to third parties.
- whether the social media account is unlinked to Morley College London.

3.3 This policy is also applicable to internal College IT systems that include social networking features, such as the College's primary internal communications tool (My Morley) and Yammer.

4. Definitions:

4.1 For the purposes of this policy, social media is defined as the type of interactive media that allows individuals to create, share and exchange content, ideas, and opinions in a public space online.

4.2 Social media can include, but is not limited to:

- Facebook
- LinkedIn
- X (formerly known as Twitter)
- Instagram

- TikTok
- Snapchat
- Pinterest
- Yammer
- Blogs (website/video)
- Social media and video/imagery sharing (e.g., YouTube, Flickr, Vimeo)
- Collaborative projects (Wikipedia, Wiki)
- Virtual social worlds
- Virtual gaming/AR worlds (eg Twitch)
- WhatsApp
- AI platforms (eg ChatGPT/Brand for creation of social media content/posts)

4.3 The term '***user'*** in this policy applies to any individual who satisfies the criteria in section 3.

4.4 ***CMEO*** refers to the Chief Marketing and Engagement Officer.

5. Statutory and regulatory requirements:

5.1 Social media use must comply with existing UK legislation relevant to social media content and publishing, which includes but is not limited to:

- Data Protection Act 2018
- UK General Data Protection Regulation 2020
- Defamation Act 2013
- Equality Act 2010
- Communications Act 2003
- Sexual Offences Act 2003
- Anti-Terrorism, Crime and Security Act 2001
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- Protection from Harassment Act 1997
- Malicious Communications Act 1988
- Copyright, Design and Patents Act 1988
- Contempt of Court Act 1981
- Offences Against the Person Act 1861
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Article 8 of the European Convention on Human Rights (listed in Schedule 1 of the Human Rights Act 1998)

6. Policy Objectives:

6.1 This policy aims to:

- Promote the responsible and respectful use of social media in alignment with Morley's values and vision;
- Minimise the risks of social media on a professional and personal basis by providing guidelines for users;
- Protect Morley College London's reputation and brand image.

7. Policy Statement

7.1 Morley College London values and recognises that staff members do actively interact and engage on social media in a personal capacity, using this to promote Morley in a positive way to followers, particularly in their area of expertise. This policy seeks to encourage and support positive promotion of the College.

7.2 The expectation of this policy is that staff behave professionally in all situations, relating directly or indirectly to the College and will conduct themselves in a way, which acknowledges the standards of behaviour expected within this and other College policies.

7.3 A user in breach of this policy may be subject to disciplinary action. A breach considered more serious, could see an individual made subject to civil or criminal legal proceedings.

8. Implementation of Policy:

8.1 Responsible Use of Social Media and Unacceptable Content

The College has no direct control over the information users choose to disclose on social networking sites. However, users must bear in mind the need to protect the reputation of the College, their own privacy, the privacy of colleagues and students and the confidentiality of College information/data in any communications or statements they make available to the public, which includes family and friends outside of Morley College London.

The College will conduct social media and online presence checks as part of its recruitment procedures in accordance with Keeping Children Safe in Education [KCSIE] guidance.

Staff must not:

- Create/ write/ publish material that might be defamatory or incur liability for the College.
- Post messages, status updates or links to material or content that is inappropriate.
    - Inappropriate content includes pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling or illegal drugs, use profanity.
    - This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone based on any protected characteristic.
- Use social media for any illegal or criminal activities.
- Disclose confidential or commercially sensitive information gained during their role at Morley.
- Send offensive or harassing material to others via social media.
- Broadcast unsolicited views on social, political, religious or other non-business-related matters.
- Use social media for advertising or endorsement purposes.
- Send or post messages or material that could damage the College's image or reputation – this extends to commenting on or reposting of others content.
- Discuss colleagues, customers or suppliers without their approval.
- Reveal any personal or identifying information of customers, suppliers, stakeholders or colleagues.
- Post, upload, forward or link spam, junk email, chain emails and messages.

8.2 Representing the College on Social Media

Only named colleagues can formally represent the College and:

- Can only use such accounts and post/ message in line with Morley's mission, vision and values;
- Encourage colleagues to use social media to promote our events, initiatives, successes, job adverts etc, sharing content from official Morley sources.

Named representatives will:

- Be respectful, polite and patient, and ensure that no post is malicious, discriminatory, libellous, offensive or defamatory.
- Be empathetic.
- Report any abusive comments or misuse immediately to the CMEO.
- Limit what they post about to matters within their expertise or role content.
- Remember that any interactions or posts can and will be shared.
- Remove offensive content and correct any inaccurate or misleading posts as quickly as possible.
- Ensure that they do not enter debate or discussion on Morley policies or processes.
- Ensure responses or posts of any kind are proportionate, relevant, and reasonable.

Should there be an investigation into actions taken through social media, regardless of outcome, colleagues should ensure that they do not:

- Monitor the posts of the other party.
- Apply likes or comments to the other posts.
- Establish "fake profiles" to continue to interact with the other party.

These steps are important to ensure that there can be no perception of ongoing harassment.

8.3 Personal use of social media

- Morley recognises the importance of social media in both a work and social environment, as such, it does not prohibit employees from accessing their personal accounts at work.
- Colleagues must act responsibly and ensure that their working productivity is not affected by using social media. It is easy to get distracted by the wealth of information available through social media, so please remain focused and keep your usage to a few minutes every day during breaks from work.
- Excessive time spent on social media for a non-work purpose could give rise to an investigation under our disciplinary or capability policies.
- Morley respects the rights of our colleagues to having a private life and to having freedom of expression. However, as Morley employees, colleagues must ensure that their personal use as an individual, whether during working time or outside of it, does nothing that can harm the reputation and / or security of the College. They must not disclose commercially sensitive or confidential information they have gained in their role with Morley or do anything that could damage Morley's reputation. Failure to follow these requirements could result in disciplinary action.
- Colleagues are asked to consider if their profiles identify their link to Morley, and where they do, they must be especially careful to follow the principles set out above at all times.

- Colleagues may wish to explicitly state that their personal accounts do not represent their employer by using a statement in their biography such as “all views expressed are my own”.
- To avoid damage to their own professional reputations we advise staff to consider what they post on social media generally in a private capacity.

Breaches of this policy will be investigated under our Disciplinary or Capability Policy.

8.4 Confidential Information

Users must not disclose confidential information, or sensitive business-related information through social media. Additionally, users must always pay due regard to the provisions of the General Data Protection Regulation (GDPR) and the Data Protection Act, and as such ensure that they do not disclose information that could constitute a breach of data protection law.

If, following an investigation, there is evidence of any unauthorised disclosure of confidential information, or action, which leads to a potential breach of data protection law, this could also lead to disciplinary action for the employee concerned.

8.5 Account Security

Users must always ensure that security information for personal and work-related accounts remains confidential, and that they do not disclose log-in information, including passwords, to people who are not authorised to use those accounts.

Where unauthorised access to an account has occurred, there is the possibility of further security breaches and potential damage to personal and/or the College’s reputation.

If a staff member believes that unauthorised access has taken place to a work-related account, they should contact the IT Services Team in the first instance for advice.

8.6 Personal safety

Staff members should take every effort to keep themselves safe, when using social media. Never post information such as postal addresses, email addresses, telephone numbers and bank details online. Users should also be suspicious of posting personal details, photographs, or details of their current location on social media sites.

Unwanted contact can be made very easily via social media sites; users should be aware and react with due care and not accept befriending invitations from strangers.

If using a shared device, users should always check that they logged off all social media sites before shutting down the device/s.

8.7 Breaches of this Policy

Social media should never be used in a way that breaches this policy, or any other College policy. If an internet posting, blog, or social media comment would breach any of the College policies in another medium, then it will also breach them in an on-line forum.

For example, employees must not use social media in a way that would:

- Breach computing regulations
- Breach social media policy
- Breach any obligations in relation to confidentiality
- Defame the College, or its affiliates, students, staff, suppliers, or other stakeholders
- Harass or bully any employee, student or third party or breach the Staff and Student Anti-Harassment and Bullying Policies

- Unlawfully discriminate against other employees, students or third parties
- Breach Data Protection Policy.

Refer to 8.1 for detailed instances of where breaches could occur.

8.8 Online bullying, harassment and victimisation

The College is committed to providing a learning environment that is free from bullying, harassment and victimisation for all students and staff. This applies to all forms of bullying, harassment and victimisation, including situations where social media is used. If users become aware that they, or others, are being bullied, harassed, or victimised on social media, they should carry out the following actions:

- Not respond directly to the comments;
- Retain evidence;
- Report the situation immediately to a line manager or Head of School or if neither of those routes is possible, an appropriate an HR Colleague

If a member of staff at the College is affected by online bullying or harassment, because of their employment at the College, relationship with staff or students, the College will provide support, guidance and if appropriate, take remedial action under the relevant policy.

8.9 Monitoring and Privacy

Users should be aware that the College reserves the right to monitor and review all aspects of use of the College IT network/s and to keep logs of individual user activity, including use of social media sites. The user concerned will not necessarily be notified that monitoring and review is taking place.

User data will normally be treated as confidential and private. However, an investigation may take place under the following circumstances:

- Requests for access/monitoring from the police or security services, as allowed by current legislation;
- Requests made under the Data Protection Act (2018) or Freedom of Information Act (2000);
- Requests to establish facts as part of a misconduct investigation under the relevant Disciplinary Policy or to establish events or particulars pertaining to a Safeguarding or Prevent concern;
- Requests from the employee themselves;
- To facilitate the operation, repair, and essential maintenance of College IT systems.

For this reason, users should not use College IT resources for any purpose they would not wish to become known to the organisation.

Please refer to the IT Systems Acceptable Use Policy for full details of monitoring and privacy in relation to the College IT and communication systems.

8.10 College maintained social media sites

Morley College London maintains official accounts for social media including Facebook, Instagram, X (formerly Twitter), LinkedIn and YouTube. Morley's corporate social media sites are managed by the marketing team and are the preferred accounts for communicating and interacting with external audiences. The social media estate also includes associated social media sites for Morley Radio and Morley Gallery, which their individual staff members manage.

It is not permitted to create social media channels that directly reference the College, without the permission of the CMEO, and for those accounts already established, the CMEO will intervene to encourage purposeful use of the channel as/when required.

Curriculum teams, with the permission of the CMEO, across the College will be responsible for the management, publishing and monitoring of content across their own social media sites and blogs that fall within their own remits. Responsibility for the suitability of information posted on college-maintained social media sites lie with the author, who must ensure that the material is appropriate for all users who might access it, including potentially, students under the age of 18 and vulnerable adults. The College will remove any content found to be inappropriate and may block users from posting on these sites if it becomes necessary.

If users become aware of inappropriate material posted outside normal working hours, they should report this to the site provider. Users should familiarise themselves with the terms and conditions of any social media sites they are using.

If staff members wish to set up a social media profile, affiliated with the College, for example using the College name or branding, they must first obtain permission from the CMEO. If the social media profile is affiliated with a specific course, the user must also obtain permission from the relevant curriculum head.

The CMEO reserves the right to audit all channels that reference the Morley College London brand, and to close or bring under corporate control any such channels in the wider interest of the College and its brand.

The Content Marketing Officer, a member of the marketing team, can give specific advice on the use of social media for the College's business.

8.11 Social Media and the End of Employment

If a staff member's employment with the College should end for whatever reason they must:

- Amend immediately any personal profiles on social networking sites to reflect the fact that they are no longer employed or currently associated with the College;
- Provide to the IT Team any relevant passwords and other information to allow access to any social media site, page or account which has been used or set up for the purpose of furthering the College's business or facilitating the provision of its curriculum;
- Relinquish any authority they may have to manage or administer any such site, page or account.

8.12 Generative Artificial Intelligence Guidance for Staff (such as ChatGPT)

Generative AIs are helpful tools that, properly used, can save time and provide assistance, insight, information and ideas for many work tasks. ChatGPT is one of the most well-known current Generative AIs available free of use to the public. Users may use AI tools to help compose their content for social media posts for example.

Staff members should have confidence to use these new tools, but in doing so, must make themselves aware of the inherent risks associated with new technologies such as AI.

Users should treat any information they give to the AI as if they were posting it on a public site, such as a social network or public blog. They should not share any personal information, company or student information, copyrighted content or any data covered by external sharing restrictions that is not generally available to the public.

Whilst AI can be an excellent tool as an auxiliary aid in creating social media content and much more, users should bear in mind that technology is rapidly evolving at pace and understand that it is fallible, and any outputs must be treated as such. Staff members can seek guidance from the CMEO if they have any questions about using AI tools.

8.13 Requests for Information

Users should not respond to requests for information from any external media outlet. Any contact made through social media from external sources regarding information relating to the college must be referred to the CMEO in the first instance.

9. Communication and Training:

9.1 This policy will be available to all staff via the College's intranet, and during induction training.

10. Monitoring and Reporting:

10.1 The Head of Marketing and Sales will review this policy every four years, or sooner if there is a notable change in legislation or technological developments.

10.2 The content marketing officer will establish a database of college affiliated social media accounts for the purpose of routine reviews and analysis of content and performance.

11. Related References, Policies, Procedures, Forms and other Appendices:

- IT Systems Acceptable Use Policy
- Data Protection Policy
- Freedom of Information Policy
- Equality, Diversity and Inclusivity Statement
- Freedom of Speech and Freedom of Expression Policy
- Disciplinary Policy and Procedure for non-Senior Post Holders
- Disciplinary and Capability Policy for Senior Post Holders
- Anti-Racism Statement
- Staff Anti-Harassment and Bullying Policy
- Student Anti-Harassment and Bullying Policy
- Safeguarding and Prevent Policy for Young People and Vulnerable Adults
- Complaints Policy and Procedure
- Public Information Policy