

Student Social Media Policy

Created: June 2018

Author: Ryan Ward

Updated by: Lisa Alden

Originating Directorate: Student and Academic Services

Approved by: Operational Leadership Group

Date of approval: September 2019

Effective date: September 2019

Due for review: June 2020

1. Introduction

- 1.1. De Montfort University (DMU) recognises the numerous benefits and opportunities that social media presents. We actively use social media to engage with students and the general public, to celebrate success, communicate research and enhance the university's profile online. Therefore, DMU also actively encourages university students to make effective and appropriate use of social media channels and to use them to engage in conversations with the DMU community.
- 1.2. Despite the opportunities presented by social media, there are risks. Social media allows individuals to communicate either in their name or anonymously with a potentially huge audience, and sometimes its informality can encourage us to be less cautious than we would be using other more traditional methods of communication and interaction. Inappropriate use of social media can be damaging to the reputation of the University as well as have a negative impact on staff and students.
- 1.3. This policy is for students and provides information on the appropriate use of social media when connected, or linked in some way, to their status as a student of the university, or when directly or indirectly referencing the university in any way.
- 1.4. This policy works alongside the following separate institutional policies and regulations:
 - General Regulations and Procedures Affecting Students, and in particular chapters 2 and 14
 - Policy on Dignity and Respect (Students)
 - Use of Computers Policy
 - Freedom of Expression
 - Academic Freedom Policy
- 1.5. The principles of freedom of expression and academic freedom apply to the use of social media; however, the university requires responsible and legal use. (See also the university's *Freedom of Expression and Academic Freedom* policy).

2. Scope

- 2.1. For the purpose of this policy, the term 'Social Media' is used to describe virtual channels dedicated to live streamed or scheduled uploads, community-based input, interactions, content sharing and collaboration through the building of virtual networks and communities. Websites and applications dedicated to forums, microblogging, social networking, social bookmarking, social curation and wikis are among the different types of social media. It also includes any other means of communicating on the internet where members of the public (including staff or students) may reasonably access the communication.
- 2.2. They currently include, but are not limited to, Facebook (and Messenger), Instagram, WhatsApp, Snapchat, Allo, Twitter, LinkedIn, Reddit, YouTube, Flickr, Pinterest, and Google+.

- 2.3. This policy applies to social media communications made both on public and private forums by students including those communications which directly or indirectly reference the University. This policy applies to social media from anywhere including off-campus and on personal devices whether to an individual, group or the world. While posts added to public forums can be seen by any member of the public from the date of publication, students are asked to remember that posts added to private forums can also be shared publicly by others. Students may be subjected to disciplinary action where they have been careless or reckless in the communication they have posted, even when they believe the forum to be private. There have been a number of high-profile cases in recent years where students across the country have been disciplined after offensive comments, made on private messaging services such as WhatsApp, were captured and subsequently shared. With this in mind, students should remember that action can be taken by the university if behaviour failing to meet policy guidelines is identified either publicly or privately.

3. Students' responsibilities

- 3.1. Students are encouraged to be mindful of how their identity, statements or views appear online and are reminded that future employers and industry contacts may view social media profiles when recruiting to gain information about a candidate's character, personality or employability. Students should therefore be conscious of publishing both texts and digital posts that may hinder them, for whatever reason, in the future.
- 3.2. Students are encouraged to review their existing social media accounts and, where appropriate, to transition to a more professional appearance. Some advice and guidance is given in Annex A.
- 3.3. All students must read and act in accordance with the principles of these guidelines, and regularly check the University's [Student Regulations webpage](#) for any minor updates to documents.
- 3.4. In addition, it is recommended that students read and act in accordance with the rules and guidelines set out by individual social media companies and providers.
- 3.5. Students should check the terms and conditions of a social media account and/or website before uploading material to it; by posting material to social media accounts and/or websites, ownership rights and control of the content may be released. For this reason, it is important to exercise caution in sharing all information, especially where the information, expressly or by implication or innuendo, identifies a third party.
- 3.6. Students must be aware of the potential impact and permanence of anything posted online. Therefore, students' should avoid posting anything that:
- They do not wish to be in the public domain
 - Contravenes sections 4, 5 and 6 of this policy.
- 3.7. Any digital material posted online could reach a wider audience than was expected or intended. Once digital content has been created and shared, there is limited control over its permanence and audience.

4. Behaviour and conduct on social media

- 4.1. Students are personally responsible for what they communicate on or through social media and they must adhere to the standards of behaviour set out in this policy and any related policies, such as Policy on Dignity and Respect Relating to Students and the General Regulations and Procedures Affecting students.
- 4.2. Students as users of social media may witness other members of society increasingly using social media for raising complaints and grievances. However, any students wishing to raise a complaint, report a crime or an incident should do so via the established university channels, e.g. [Student Complaints Procedure](#), or by contacting the Police; they should not raise complaints or air grievances via social media. This is the fastest way to get a response and resolution to your problem. Students should contact the university and/or the Police as soon as possible, saving any evidence, e.g. screenshots of social media. Remember that by airing any grievance or complaint publicly, it may limit any action that can be taken and can lead to civil action against the author if the complaint is found to be false.
- 4.3. Use of social media must not infringe on the rights, or privacy, of other students or staff and students must not make ill-considered comments or judgements about other students, staff or third parties.
- 4.4. We recommend that permission to share third party material, including all images, photography, text and videos, should be sought and recorded in a tangible format before uploading them to or linking them via social media. Furthermore, where permission is obtained, we recommend such materials should be credited appropriately. Guidance can be obtained from the Library website at <http://library.dmu.ac.uk>
- 4.5. The following non-exhaustive list is considered to be of an unacceptable nature and should never be posted:
- Confidential information (which may include research not yet in the public domain, information about fellow students or staff or personal matters, non-public or not yet approved documents or information)
 - Details of complaints/potential complaints and/or legal proceedings/potential legal proceedings involving the University
 - Personal information about another individual, including contact information, without their express permission
 - Comments posted using fake accounts, made-up names or using another person's name without their consent
 - Inappropriate material, including but not limited to images, that is, or may be perceived to be threatening, harassing, discriminatory, illegal, obscene, indecent, defamatory, or hostile towards any individual, group or entity
 - Any other posting that constitutes, or may constitute, a criminal offence
 - Anything which may bring the University into disrepute or compromise the safety or reputation of colleagues, former colleagues, students, staff and those connected with the University.

- 4.6. Students should be mindful that statements on social media that cause harm to an individual, including to their reputation, or that interfere with an ongoing disciplinary/legal process may create a potential claim against the individual making the statement. Furthermore, this may extend to the sharing of statements made by others.
- 4.7. Students should also be aware that communications on social media are also subject to legislation, which aim to prevent interference with legal proceedings regardless of intent to do so.
- 4.8. An individual, including the complainant, may undermine proceedings or processes by publishing information, including imagery, relating to existing or potential complaints and/or legal proceedings. This may be done in the heat of the moment; however, students should be aware that by doing so they might bring the university into disrepute or compromise the safety of the university community. As such, this conduct may be seen to be of an unacceptable nature, as per paragraph 4.5 above.
- 4.9. Students, and student groups, e.g DSU societies, must take particular care not to state or imply that their views are those of DMU when using social media, nor use the University logo at any time.

5. Cyber bullying

- 5.1 The University will not accept any form of bullying or harassment by or of members of the University, students or stakeholders or visitors, e.g. De Montfort Student Union. Additional information can be found in Chapter 2 of the General Regulations and Procedures Affecting Students and the Dignity and Respect policy and the Information Security policies and guidelines, found [here](#).
- 5.2. The following non-exhaustive list of examples illustrate the types of behaviour, displayed through social media, which the University considers to be forms of cyber bullying:
 - Maliciously, negligently or recklessly spreading rumours, lies or gossip
 - Intimidating or aggressive behaviour, as perceived by those viewing the social media
 - Offensive or threatening comments or content, as perceived by those viewing the social media
 - Posting comments/photos etc. deliberately, negligently or recklessly mocking an individual with the potential to harass or humiliate them, as perceived by those viewing the social media.
- 5.3. Cyber bullying may also take place via other means of electronic communication such as email, text, instant message, video, audio or images – edited or otherwise.

6. Students use of official university accounts

- 6.1. Some students may contribute to the university's official social media activities as part of their role, for example taking over the Snapchat or Instagram accounts, vlogging, writing

blogs or running an official Twitter account. Students should be aware that while contributing to the university's social media activities they are representing the university.

- 6.2. Misuse of official University accounts may lead to suspension and, following a disciplinary committee, may lead to expulsion; students will not be eligible for readmission to the University at any time in the future as per Chapter 2 of the *General Regulations and Procedures Affecting students*.

7. Breach of the policy

- 7.1. If a student is found to have acted in breach of this policy this may lead to consideration of disciplinary action being taken against them in accordance with Chapter 2 of the *General Regulations and Procedures Affecting Students*.
- 7.2. Any individual suspected of committing a breach of this policy will be required to cooperate with any investigation in accordance with the disciplinary procedure. Non-cooperation may lead to further disciplinary action in accordance with Chapter 2 of the *General Regulations and Procedures Affecting Students*.
- 7.3. Any individual may be required to remove internet or social media posts that are found by the university to be in breach of the policy. Failure to comply with such a request may result in further disciplinary action.
- 7.4. Any breach of this policy must be reported in line with DMU's [Student Complaints Procedure](#). In the first instance, any breaches must be brought to the attention of the DMU Security Team by email at security@dmu.ac.uk or by phone on (0116) 257 7642.

8. Monitoring

- 8.1 The university will:
- Ensure this policy, and any changes, is accessible to staff and students
 - On occasion, provide guidance for students on how to stay safe online when using social media. Initial guidance is available at Annex A. Further guidance on [Staying Safe Online](#) is available from ITMS.
 - Monitor references to the university on social media and the internet and respond to complaints regarding student conduct on social media
 - Take disciplinary action where inappropriate behaviour is exhibited that affects students, staff, the University or members of public in accordance with the university's *General Regulations and Procedures Affecting Students*, and in particular Chapters 2 and 14 of those Regulations.
 - Annually review and update this policy, where appropriate, and any other associated policy and guidelines and publish details of any changes.

Annex A – How to use social media

How to use social media

Tips and hints on staying safe and managing your reputation

We all recognise the enormous benefits and opportunities that social media presents and we actively encourage our students to use social media to communicate and keep in touch with latest news and research in their area.

Despite the opportunities, there are risks. Social media allows individuals to communicate with a potentially large audience, and sometimes its informality can encourage us to be less cautious than we would ordinarily be.

These tips are to help you when you are considering posting on social media. They will help you manage your professional reputation and ensure you follow university guidelines and the law.

The Centre for Enhancing Learning through Technology (CELT) are able to provide support and guidance for users of various social media technologies.

- **Remember, everything you post online is public.** Once it's out there you lose control of how others might interact with it. Posting anything online (even on closed profiles or private messaging services, like WhatsApp, for example) has the potential to become public, even without your knowledge or consent.
- **Think before you post.** Would you be happy for your family, lecturer or future employer to see it? If not, then it's probably not a good idea to post it. There have been a number of high profile cases where students across the country have been disciplined after offensive comments made on private messaging services, like WhatsApp, were captured and subsequently shared.
- **Consider how the content of your messages may appear to others.** Offensive materials, including text, images and video, have the potential to cause serious upset and severely damage your professional and personal reputation. Consider how others may perceive your content. How could a potential employer view the content? **Employers are increasingly checking the digital footprint of potential staff.** This means looking at old tweets, posts and comments on forums. Will sharing the content result in you falling short of expected standards at university and the law? If so, it could result in the university taking disciplinary action. Don't forget, it can be hard to take something back once it has been shared, copied, or redistributed.
- **Check your privacy settings.** Protect your personal information and that of others that could be misused. Think about who can see your address, telephone number, date of birth and email address. And, definitely don't share your bank details online. Also remember that while you may be sharing the content privately (on your own private profile or in a private forum) others can share that content publically if it is available.

- **Use Secure Passwords.** Remember to use a secure password and current advice for this is to use a pass phrase of three or more words that you can picture in your head. Never re-use passwords across different websites. Where possible use second factor authentication methods, which may include sites sending an SMS or an authenticator app on your phone. For further information see <https://www.getsafeonline.org/protecting-yourself/passwords/>
- **Make sure you familiarise yourself with expectations regarding professionalism and confidentiality on your course**, especially if your course is accredited by a professional body. If you breach the code of conduct of a professional body, it is very likely to affect your ability to study and your future career.
- **Be aware of sharing third-party materials.** Do you need permission to share the materials or should you, as a matter of courtesy, contact the party? Make sure you check before posting as infringement of rules could break copyright and/or intellectual property laws.
- **Finally question everything you read online.** Not everything you read might be completely accurate. Who wrote it? Where did it come from? Does the imagery look poor quality? If you think it looks or sounds inaccurate, it's probably best avoided. Writing and distributing inaccurate statements about people and organisations can be unlawful and lead to legal action.