

Social media guidelines for students

1. INTRODUCTION

The University is dedicated to creating and maintaining a safe, welcoming, inclusive and diverse community that nurtures a culture of mutual respect and consideration. This applies to all environments including social media. All members of the University community must be able to thrive within their roles without fear of any form of inappropriate behaviour, including online harassment.

For the purposes of these guidelines, the term 'Social Media' is used to describe dynamic and socially-interactive, networked information and communication. Example sites include, but are not limited to:

- Multimedia and social networking sites, such as Facebook, LinkedIn and YouTube
- Internal or external blogs and micro-blogs including Twitter
- Community discussion forums such as Yahoo! Groups and Google Groups
- Review or ratings forums such as TripAdvisor, BBC Have Your Say and MoneySavingExpert
- Wikis, such as Wikipedia
- Any sites where you can post text, photos and video, such as Pinterest, Flickr, Google+, Tumblr

The University of Cambridge has a number of official accounts on sites such as Facebook, Twitter, YouTube and Instagram where the opinions expressed and information shared reflects the views of the University as a corporate body. Any student (either on an individual basis or as a group) seeking to set up a formal University of Cambridge social media account (or any featuring the University logo) should seek prior permission from the Office of External Affairs & Communication.

2. PURPOSES AND OBJECTIVES

These guidelines are designed to provide advice and guidance to University of Cambridge students who are using (or considering using) social media in any capacity. It has been compiled to assist students to understand the reputational, legal and ethical implications of engaging in online communications of this nature, what can happen if social media is misused, and how to safeguard students' wellbeing, personal security, current/future career prospects and the reputation of the University.

3. PRINCIPLES

3.1 General responsibilities

- It is the responsibility of students to:

- read and act in accordance with these guidelines, and any additional guidelines published by your College
- read and act in accordance with the rules and guidelines set out by individual Social Media, Social Networking and Website Hosting companies and providers
- Consult with your College and where relevant seek ethical approval before posting, as part of your studies / research, pictures, videos or comments through social media that could be viewed as offensive or as bringing the University into disrepute.
- It is the responsibility of the University to:
 - ensure these guidelines are highlighted at student induction sessions, or at some other relevant time in the academic year
 - ensure these guidelines are accessible to
 - monitor the University of Cambridge social networking sites and remove inappropriate content

3.2 Responsibilities of students in official University online/social media presence (eg Instagram takeover of a main University account)

- Remember that you are representing the University at all times when posting comments or responding to those made by others.
- Social media sites should not be used for raising and escalating concerns relating to your course, the University or any members of the University. Seek advice from your College if you have any concerns.
- Ensure that you do not reveal confidential information about the University or its staff, students, partner organisations or clients.
- Comply with relevant professional codes when using social media as part a research study or project.
- Ensure you do not use your site or pages in any way that may compromise your current or future fitness to practice or employability.
- Obtain permission from the Office of External Affairs & Communication before using the University's brand.
- Consult the Office of External Affairs & Communication if there is any media interest resulting from your online activity.

3.3 Responsibilities of students in personal online/social media presence

- Be aware that third parties including the media, employers and Police can access profiles and view personal information. This includes pictures, videos, comments and posters. Inappropriate material found by third parties affects the perception of the student and the University and can have a negative impact on a student's future prospects.
- Communications made in a personal capacity through social media must not:
 - be unlawful – i.e. breach any UK criminal and/or civil legislation,
 - include anything that could be considered discriminatory against, or bullying or harassment of, any individual. This includes:

- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age
- using social media to harass another individual or
- posting images that are discriminatory/offensive or links to such content
- encourage illicit drug-related activity. This includes but is not limited to posting pictures, videos or comments that promote or portray the personal use of drugs and drug paraphernalia
- depict or encourage unacceptable, violent, illegal or dangerous activities e.g. sexual harassment or assault, fighting, vandalism, academic dishonesty, drunk and disorderly behaviour, drug use etc through posting pictures, videos or comments
- breach copyright eg using someone else's images or content without permission; failing to give acknowledgement where permission has been given to reproduce something
- breach confidentiality eg revealing confidential information owned by the University; giving away confidential information about an individual or organisation
- use the University's logo on personal social media sites

You also need to be aware of a number of other relevant policies and guidelines:

- Student Rules of Behaviour (www.studentcomplaints.admin.cam.ac.uk/student-discipline)
- Data Protection Policy (www.information-compliance.admin.cam.ac.uk/files/data_protection_policy_final.pdf)
- Dignity at Work Policy (www.hr.admin.cam.ac.uk/policies-procedures/dignity-work-policy)
- Computer Regulations (<https://help.uis.cam.ac.uk/policies/governance-and-policy-documents/use-and-misuse-of-computing-facilities>)

4. MISUSE OF SOCIAL MEDIA

- The University has the right to request the removal of content from an official social media account if it is deemed that the account or its submissions pose a risk to the reputation of the University or to that of one of its members
- Students who post views, opinions or images online in breach of these Guidelines may be subject to disciplinary action. Such actions may also be subject to prosecution under UK criminal and civil legislation
- Prospective employers may trawl social media sites as part of their selection process and the social media posts that you make could undermine your future employment prospects

5. STAYING SAFE ONLINE

- Only post publicly what you would be happy for journalists, lecturers and prospective employers to see/read
- Remember that everything you post online is public, even with the strictest privacy settings. Once something is posted online, it can be copied and redistributed, and it is easy to lose control of it. Presume that everything posted online will be permanent and will be shared
- Think before you send. Avoid posting anything when you have been drinking or are feeling angry – you may regret it the next day but it could be viral by then
- Remember that what is a 'joke' to one person may feel like bullying and harassment to someone else. The University doesn't tolerate bullying and harassment. If you feel bullied online, seek advice from the Office for Student Conduct, Complaints and Appeals (OSCCA@admin.cam.ac.uk)
- Be aware that posting 'jokes' has led some people to be prosecuted and even imprisoned. Don't post things that may be considered offensive or make 'joke' threats
- Ensure that you protect your personal information and that of others that could be misused (eg home address, telephone number, date of birth)
- Think about who you want to be able to see your information and set privacy settings accordingly. Remember that even with strict privacy settings, others can share your posts so you have no control over who sees them
- Don't say or write anything that could have a negative impact on the reputation of anyone or any company. Any statement which could have a negative impact on a person (or business's) reputation could lead to accusations of libel / defamation and lawsuits
- Be very cautious about arranging to meet someone you only know online. They may not be who they say they are. Arrange to meet during the day in a public place and take a friend or tell friends where you are going

6. DON'T GET ADDICTED

Did you know?.....

- Negative mood, depression, attention deficit and hyperactivity disorder, as well as social isolation, low self-esteem and psychosis are all associated with internet addiction
- Smartphone users check their phones 150 times a day on average
- Phone addicts are often easily distracted, suffer disrupted sleep and are tempted to lie about their phone use
- Overuse of a smartphone can lead to a range of physical and psychological disorders

So what can you do?.....

- Schedule your internet time and keep parts of the day 'internet free'
- Don't use the internet in bed just before you sleep or during meals

- Accept that you don't have to answer every email/text message immediately
- Disable unnecessary notifications
- Make the internet work for you, don't become dependent on it for your peace of mind

7. FURTHER INFORMATION

The following links have useful information on keeping safe and other issues:

- The Information Commissioner's Office's social networking guidance - includes how to set privacy settings: <https://ico.org.uk/your-data-matters/be-data-aware/social-media-privacy-settings/>
- Cambridgeshire Constabulary Internet Safety Guide: <https://www.cambs.police.uk/information-and-services/Online-safety/Internet-safety>
- University of Cambridge's Breaking the Silence anti-harassment website: <https://www.breakingthesilence.cam.ac.uk/>

8. RELEVANT EXTERNAL LEGISLATION

- Data Protection Act 1998
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000.
- Freedom of Information Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- The Terrorism Act 2000
- The Anti-Terrorism, Crime and Security Act 2001
- Obscene Publications Act 1994