UNIVERSITY OF CAMBRIDGE

Social media guidelines

Version 1.4
Last updated 20 April 2016

Context

We (the Office of External Affairs and Communications) recognise the numerous benefits and opportunities that a social media presence offers. We aim to build relationships and work with collegiate Cambridge to share information about the University's activity online, and how to better support it. We will actively use social media to engage the public, communicate research and enhance the University's profile online.

Social media accounts provide a flexible delivery platform. Our office actively encourages University staff to make effective and appropriate use of them; and to engage in conversations with colleagues and the community.

We've written these guidelines to help staff plan, setup and manage social media accounts. They should be read alongside related University policies:

- Policy on the acceptable use of computer facilities, email and the internet
- Use and Misuse of Computing Facilities (taken from rules made by the Information Services Committee)

Authorisation and Review

These guidelines were originally published in July 2014. The latest version was updated in January 2016 and approved by the Director of Communications.

You can email questions relating to this guidance to Digital Communications.

The impact of this guidance will be monitored regularly to reflect the changing online environment and technologies. The guidance may also be amended where particular concerns are raised or where an incident has been recorded. Institutions within the University that wish to run social media accounts should designate one of their staff as their Social Media Champion. It is the experience of the appointee, not the title that is important. Ideally, the named individual selected should have knowledge of how social media works, a clear understanding of the institution's approach, practices and guidance, and the ability to deliver effective training.

Scope of the guidance

For the purposes of this guidance, social media is defined as any online interactive communication tool which encourages participation and exchanges. Common

examples include; Twitter, Facebook, YouTube, Instagram and LinkedIn.

This guidance is for all staff who directly or indirectly, represent the University online. It applies to online communications posted at any time and from anywhere, whether to an individual, a limited group or the world.

Personal vs professional profiles on social media

The University respects privacy and understands that staff may use social media accounts in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the institution's reputation are considered in this guidance.

Professional responsibilities apply regardless of the medium being used. All social media communications that might affect the University's reputation, whether made either in a private or professional capacity, should be thought through carefully.

Professional communications are those posted through an institutional account.

Personal communications are those made via a private social media account. Where a private account is used which clearly identifies the University of Cambridge as your employer it must be made clear that the member of staff is not communicating on behalf of the University. An appropriate disclaimer, such as:

"the views expressed here are my own and in no way reflect the views of the University of Cambridge" should be included.

If you or the content that you post links you to the University, expect that it could be re-published by the national or international press and by proxy, attributed to the University.

Private communications that do not refer to the University (either implicitly or explicitly) are outside the scope of this guidance.

The University and Colleges are strongly committed to the principle of freedom of speech and expression, and this includes interactions through social media. It should be noted, however, that social media is a tool known to be used by terrorists to encourage others to adopt extreme beliefs or attitudes. All members of the University that use social media are therefore expected to use it responsibly. The University and Colleges take seriously their requirement to report content or views that promote or incite criminal extremist behaviour on their social media platforms or as a result of the misappropriation of their brands. Members of the University should report such concerns to the Head of Digital Communications and email prevent@admin.cam.ac.uk.

UNIVERSITY OF CAMBRIDGE

Feedback and further information

We welcome all constructive feedback on this and any other guidance. If you would like further information on social media, or wish to send us your comments on our Social Media Guidance, then please contact Digital Communications.

Setting up new accounts

You are welcome to create social media accounts on behalf of your institution providing that:

You have a clear understanding of:

- ☐ The University's Social Media Guidelines (these guidelines)
- ☐ Who the new account is aimed at
- ☐ The type of content you are going to post via the account and how you are going to produce it
- ☐ The mechanics of the network that you are creating an account on, and the expected behaviour and publishing patterns of people that use it

You agree to:

- ☐ Let your institution's Social Media Champion know the name of the account, and what you're going to use it for
- ☐ Conform to the University's brand guidelines. If you need help with creating artwork for the account, the University has provided a set of Social media templates
- ☐ Set the account up in such a way that multiple people within your institution can share the load of running it, or that if a staff member who setup the account leaves, access to the account is still possible. This could be done by:
    - Using a role rather than email address to sign up for the account (providing all those that have access to the address have read this guidance and can help run the account responsibly)
    - Setting the account up with a backup email address using a role address

Roles and responsibilities

As mentioned previously, we've referred to an individual in your institution as a Social Media Champion. This is a placeholder title, feel free to use what you will but the key is that there should be a named (and known) individual in your institution that can be a go-to for social media expertise and advice.

Designated Social Media Champions should try to:

- Keep up to date with technology developments through appropriate personal and professional development
- Review and update all relevant local documentation
- Deliver or signpost training and guidance on social media
- Take a lead role in responding to and investigating any reported incidents
- Make an initial assessment when an incident is reported and involve appropriate staff and external agencies as required
- Maintain a directory of local social media accounts

All staff are responsible for:

- Knowing the contents of this guidance
- Attending appropriate training
- Informing the Social Media Champion where an institutional account is to be used
- Regularly monitoring, updating and managing content he/she has posted via local accounts
- Reporting any incidents in line with guidance in this document "Incidents and response"

Line Managers are responsible for:

- Addressing concerns or questions regarding posts or comments via official and personal accounts
- Reporting outcomes to the Social Media Champion, or escalating the matter to involve appropriate agencies
- Attending additional relevant training

Behaviour

The Office of External Affairs and Communications recommends that all staff using social media adhere to the standard of behaviour as set out in this guidance.

Staff should not use social media to screen job applicants or students as part of the recruitment selection process. In addition, social media should not be used to screen potential donors. However, it is fine to use social media to promote vacancies (the HR team have a policy in place for this). Staff should not use social media to infringe on the rights and privacy of colleagues or make ill-considered comments or judgments about staff.

Digital communications by staff should be professional and respectful at all times and in keeping with this guidance. Where an incident is reported, refer to Incidents and response.

Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing

content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the University of Cambridge and will be reported as soon as possible to a relevant member of staff, and escalated where appropriate. The University will take appropriate action when necessary.

Where conduct is found to be unacceptable, the University will deal with the matter internally. Where conduct is considered illegal, the University will report the matter to the police and other relevant external agencies, and may take action according to the Disciplinary Policy.

The University permits reasonable and appropriate access to private social media accounts. However, where we suspect excessive use, and consider this use to be interfering with relevant duties, we may take disciplinary action.

The following general guidelines apply to staff posting content via social media:

Do:

- Check with a line manager before publishing content that may have controversial implications for the institution
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Manage your social media account(s) on behalf of the University
- Think before responding to comments and, when in doubt, get a second opinion
- Set up a shadow system i.e. a colleague who can edit posts
- Seek advice and report any mistakes to your line manager

Don't:

- Don't make comments, post content or link to materials that will bring the University into disrepute
- Don't use University branding on personal accounts
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content, and don't link to, embed or add potentially inappropriate content
- Don't use social media to air internal grievances

UNIVERSITY OF CAMBRIDGE

Content for social media accounts

Consider a publishing strategy

- Decide what information will be shared through your social media accounts. Is it used to promote future events, help with general communications or student applications?
- Decide if updates include University-wide happenings or just departmental ones
- Create a timetable for all departmental events which you plan to promote via your social media account(s)
- Updates should not breach e-safety; the use of names should be omitted
- Are you going to use the account to respond to enquiries or just to push out content? If the former, then make sure you can respond within a few hours

Persona and tone of voice

It is recommended to have a consistent voice, if multiple users are producing content for a departmental social media account. To help maintain consistency:

- Speak in first person plural: “We are holding an event tomorrow. Feel free to contact us.”
- Try to use active, rather than passive, words
- Try to maintain a semi-casual tone, without using slang or jargon

Suggestions for department-related updates

- Any major updates made to the departmental website
- Reminder of an up-and-coming event or a registration deadline
- Photos from events (departmental or University)
- New videos, research findings
- Forum/discussion questions that are posed to followers

Promoting your accounts

There are a few simple steps that can be taken to promote departmental social networking sites in a subtle but effective way:

- All emails sent from the department should include a hyperlink to its social media account(s). The hyperlink(s) should be included in the email signature
- Any mailings could highlight the department’s social media accounts
- Presentations should include details of the social media accounts in the ‘how to contact us’ section

- Your departmental webpage should clearly signpost your social media accounts
- Following an event, encourage participants to view photos/video clips on your social media accounts

Response monitoring and management

- Checking for new queries or responses should be done a few times a day. In general, social media users don't expect an instant reply but queries should be acknowledged in a timely manner to maintain users' confidence
- Responses to queries should give a short answer to an exact question posed, with a link to relevant information on an appropriate website
- Avoid giving the impression that questions are foolish, or that information should have been easily found elsewhere
- Make appropriate arrangements when people responsible for replying to the queries are on holiday
- Publish your moderation policy
- In line with page 22 of guidance from the Information Commissioner's Office, Freedom of Information (FOI) requests made through your institutional social media accounts, which include the sender's real name, should be dealt with in the same way as an emailed FOI request. If the user's real name is not obviously identifiable from their social media profile, you should provide guidance on how to make a genuine FOI request.

Security

Security

Staff are responsible for ensuring that passwords and other access controls for University social media accounts are of adequate strength and kept secure. Passwords should be regularly changed in consideration of Information Services' guidance on passwords and under no circumstances, should passwords be shared. Staff should be familiar with privacy settings and ensure that these are appropriate for both content and intended audience.
When making use of social media accounts there are various security risks to address. Staff should be aware of the risk of false information being posted on the institution's behalf, where an account is hijacked for example. When logged into a social media account you are exposed to having your account hijacked if you click on a phishing link. These are often disguised as genuine enquiries or comments for example "Look what someone is saying about you [hyperlink]". If in doubt check with the Cambridge Computer Emergency Response Team (CamCERT).

Staff should ensure that any devices that have social media login details stored on

them are set to lock automatically after each use. If any devices which contain login details are lost or stolen, staff should change the passwords of all social media accounts that the device was connected with, and let other managers of the accounts know.

Use of other people's materials

Sharing content such as images, photographs and video is extremely popular and easy to do via social media accounts. While this may have value in an educational context, there is a real risk of breaching the rights of individuals who own the different media e.g. images rights, patents, copyright in a blog, or rights associated with collaborative outputs. All staff should ensure they have permission or other justification to share content in this way. Content is particularly risky where it is commercially valuable, confidential and/or sensitive.

Staff will not post any images, photographs, videos, text etc. via social media accounts without appropriate permission from the rights holders. If unsure, staff are advised to check permissions attached to digital content prior to posting via social media.

Liking and sharing relevant posts from other user's social media accounts is good practice. It shows that your account is giving back to the community and not just broadcasting its own messages. However, you should validate the authenticity of any users that you would like to share content from paying particular attention to:

- Fake accounts which are set up to represent individuals that don't have their own official presence on a network
- Spam or automated accounts which exist to increase follower numbers but don't have an authentic voice, these can often be spotted on Twitter by a high equal number of followers and accounts followed (many thousands of each)

Further information and guidance is available from Legal Services.

Personal information

Personal information is information about a particular living person (which includes photography or other recording media). No personal information will be shared via social media accounts without consent, unless it is in line with our Data Protection Policy. Authorised staff posting content or setting up accounts are responsible for ensuring appropriate informed consents are in place. Members of staff should include their name, email and job title where possible. It is at their discretion whether they wish to post additional contact information.

Staff must keep colleagues' personal information safe and secure at all times. When using social media accounts, staff should never publish colleagues' personal

information. By its very nature, social media enables and encourages users to share data, including personal data e.g. a photograph of an identifiable living person. The University must process all personal information that it collects and uses in compliance with the Data Protection Act 1998. All uploads, storage, communications must be lawful and fair. Staff intending to use a social media account must therefore ensure that all parties know what type of information they are expected to share, for what purpose and who will have access to it. Even where consent is in place to process personal data, staff must also ensure that adequate security is in place to protect it. Information may range from name, registration number to sensitive personal data relating to personal experiences or assessed work.

Education and training

The Office of External Affairs and Communications wishes to make it clear to staff what our guidance contains and the reasons behind it. We will provide staff with additional guidelines and training, and the Social Media Champions will be on hand to answer any queries and address any comments.
Staff who use University social media accounts, should seek training on relevant safeguards and acceptable practice. New, or temporary members of staff, should also receive this training as part of the induction process.
Additional training is offered to senior staff and heads of department on the management of social media accounts. It is expected that all relevant staff will attend at least one session per academic year.

Incidents and response

The University will act immediately to prevent, as far as reasonably possible, any damage to an individual, their rights or the institution's reputation. Any stakeholder or member of the public may report an incident to the institution. This should be directed immediately to Social Media Champions, line managers or if needed Digital Communications. Where it appears that a breach has taken place, the Social Media Champion will review what has happened and decide on the most appropriate and proportionate course of action. Where the Social Media Champion considers the incident to be serious, this will also be reported to the Head of Department.
Where staff are in receipt of offensive, unacceptable content via social media, this should be reported to a relevant line manager immediately.
Where questionable content has been sent to the institution, the Social Media Champion should be informed prior to any response being submitted.

Moderation

Many social networks offer an opportunity for members of the public to comment below content that you have posted on behalf of the University. We would advise

against letting this go un-checked, and indeed ideally you should follow and implement a moderation policy. As an example, this is the moderation policy we use to manage our Facebook page:

The University of Cambridge welcomes the community's contributions to the online discussion environment on its Facebook Page (e.g. comments, photos and photo tagging).
This page provides a place to discuss the University of Cambridge; its research, events and breaking news. The following guidelines are designed to help provide a quality environment for our fans. Please take a minute to read them and keep them in mind whenever you participate.
The University of Cambridge abides by Facebook's Terms and Conditions, and the University asks its Facebook Fans to do the same. In particular, please do not "post unauthorised commercial solicitations (such as spam)"; "bully, intimidate, or harass any user"; "post content that is hateful, threatening, pornographic, or that contains nudity or graphic or gratuitous violence"; or "do anything unlawful, misleading, malicious, or discriminatory" on the University of Cambridge's Facebook Page. It is important to note that all comments and postings by fans on this site ("User Content") do not necessarily reflect the opinions of the University of Cambridge.
The University of Cambridge reserves the right to remove any posts that contain commercial solicitations; are factually erroneous/libellous; are wildly off-topic; or that otherwise violate Facebook's Statement of Rights and Responsibilities.

Social media templates

Because of the University's high profile and the large amount of people who connect with it online, certain rules should be followed to portray a unified and cohesive brand.

Two templates have been created to help users create social media artwork with ease and speed. These can be found at http://www.cam.ac.uk/socialmediaguidelines

If you have any queries contact the Digital Communications Team.

Measuring success

You should regularly audit which accounts you are running and understand:

- How often you are able to post content to them
- Whether the content that you post results in any meaningful engagement with users

If the answers to these two questions is "very rarely" and "no" you should consider closing the account down or focus more resource on running the account. If you

would like an assessment of what's working and what isn't please email the Digital Communications Team.