Social Media Policy

1. Purpose

Girton College ("College") recognises the importance and the numerous benefits and opportunities a social media presence offers. The College uses various social media platforms to raise the College profile by building relationships and engaging with College members, alumni and the public; to promote and communicate news and research pertaining to College life. However, the risks of using such wide-ranging and instantaneous communication tools, can have a profound impact upon the reputation of College and its members.

The Social Media Policy describes the purpose, acceptable use and management of social media platforms and accounts by staff and members of the College to ensure it meets all relevant regulatory and legislative obligations, in both personal and work life.

The College as a collegiate member of the University, accesses the internet via the University's Data Network. Therefore, this policy should be read in conjunction with the rules, guidance and disciplinary procedures set by the Information Services Committee[1].

2. Scope

This policy applies to all staff and members[2] of the College where they are acting on behalf of the College in the course of their duties as employees or volunteers. The policy is also applicable to all students, consultants and third-party agents who have access to and are responsible for the communications on College Social Media platforms.

Social Media Platforms, in the context of this policy, refers to any online interactive communication tools which encourages individuals and organisations to interact and exchange views. This will include community message boards and chat rooms hosted on the CUDN, and any external platforms which currently include but are not limited to Facebook, Instagram, LinkedIn, Viva Engage (formerly Yammer) X (formerly Twitter), and YouTube.

3. Legislative and Regulatory Obligations

The College as a Higher Education establishment is subject to the following legislative and regulatory obligations in relation to information and information systems:

The legislation includes, but is not limited to:

- Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR)
- Freedom of Information Act 2000
- The Counter-Terrorism and Security Act 2015 (PREVENT duty)
- Higher Education (Freedom of Speech) Act 2023
- Regulation of Investigatory Powers Act (2000) (RIPA)
- Privacy and Electronic Communications Regulations 2003
- Human Rights Act (1998)
- Copyright Designs and Patents Act (1988)
- Computer Misuse Act (1990)
- Equality Act 2010

4. College Information Policies

This policy should be read in conjunction with, but not limited to:

- Data Protection Policy

[1] https://help.uis.cam.ac.uk/policies/governance-and-policy-documents

[2] Appendix A - Definitions

- Data Privacy Statements
- Information and Records Management Policy
- Records Retention Schedules
- Information Governance Policy
- Email Acceptable Use Policy
- IT Acceptable Use Policy
- College Statutes, Ordinances and Regulations
- Employment handbook and Personnel Manual
- Staff-Student Personal Relationships Policy

5. Principles and obligations

5.1. Communicating on behalf of the College

5.1.1. Some individuals working for or on behalf of the College will, by the nature of their position or role, be knowledgeable or have the necessary expertise about aspects of the College, which permits them to speak on behalf of the College.

5.1.2. Individuals must only speak on behalf of the College if they have been authorised to do so – in writing – by their head of department.

5.1.3. Individuals should never falsely represent themselves or the College, nor provide misleading information. Any statements or information shared on social media must be accurate and any claims made must be substantiated.

5.1.4. Individuals must be transparent and clearly identify themselves on social media, stating their role at the College. All individuals representing the College must and will be held accountable for any information shared online. (see the **Social Media Guidance** for further information).

5.1.5. Individuals must not impersonate other members of College, nor post online anonymously or using pseudonyms.

5.1.6. Only publicly available statements or information – which has been authorised for dissemination – may be shared on social media platforms. Confidential, commercially sensitive or proprietary information should **never** be shared.

5.1.7. Individuals should refer to the relevant department and/or the Communications Officer before responding to, or entering into, social media discussions that relate to confidential and/or sensitive information.

5.1.8. Individuals should not endorse any products, services, groups or societies that conflict with the core values and principles of the College, particularly those which pose a risk to the reputation of the College.

5.1.9. College social media accounts should be only created with the permission of the Communications Officer, who shall always have access to and monitor the account.

5.1.10. Individuals should ensure that they have obtained the appropriate permissions to publish third party details or material online, in accordance with data protection legislation and/or copyright legislation.

5.1.11. Individuals with the management or administrative responsibility for College social media accounts must ensure account details are secured using a strong password and multi-factor authentication, in accordance with the College's Password Policy.

5.1.12. Account details must be updated immediately as a result of a security breach or where a social media account administrator leaves.

5.2. Acceptable use and monitoring

5.2.1. Individuals should not create personal social media accounts using their Cambridge email address (unless they are creating/moderating an official College presence on the respective social media platform). Cambridge IT accounts are provided primarily for academic and related work activities – although it is recognised that these accounts may be used for a limited personal use.

5.2.2. In accordance with the College's Staff-Student Personal Relationships policy, individuals should avoid situations which would undermine their professional responsibility or a position of trust. Therefore, individuals should seek guidance before engaging with, "following", or otherwise interacting with current students via personal social media accounts.

5.2.3. Individuals who use the College IT facilities and equipment to access social media for either work-related purposes or personal use, will be subject to the University's IT Regulations[3].

5.2.4. Individuals should be aware of the security threats social media poses. Accounts and devices must be appropriately secured and use mitigating measures, such as multi-factor authentication, wherever possible. Where information is distributed via an insecure social media account or device – the individual will be accountable for any breach or misconduct that occurs.

5.2.5. Where appropriate, the College and University reserves the right to monitor the use of social media platforms, in accordance with relevant legislation, and take appropriate action to protect against any misuse that may be harmful to the College or its members, or that is deemed unlawful. This includes but is not limited to sharing:

- malicious content e.g., trojans, viruses, worms
- illegal content e.g., any comments, data, images, video or other material which includes but is not limited to:
    - pornography, terrorism/extremism, libellous or defamatory material
- offensive content which constitutes bullying and harassment e.g., any comments, data, images, videos or other material which includes but is not limited to:

[3] https://help.uis.cam.ac.uk/policies/governance-and-policy-documents/use-and-misuse-of-computing-facilities

- race, gender, disabilities, age, sex, sexual orientation, religious beliefs and practices, political beliefs or nationality
- commercial activities or advertising material
- copyright material of another person or company

5.2.6. Where an individual's use of social media is considered to breach the College's policies and/or the University's IT Regulations, the College will take disciplinary action in accordance with current policies and procedures.

5.2.7. Disciplinary action will be determined on the perceived risk and impact to the College and the nature of the offence. Individuals will be asked to remove any content posted on social media – even if in a personal capacity – which breaches the College's Policy and the University's IT Regulations. A refusal or failure to comply may result in disciplinary action.

5.2.8. Social networking sites and the content posted by individuals (which may include comments, videos, or photographs, which have been posted on social media sites about the College and its members), may be referred to in any subsequent investigations of possible misconduct. Where applicable, misconduct or breaches which are illegal may be referred to the appropriate legal authorities (e.g., Police).

6. Reporting Incidents

6.1. For any suspected breaches of this policy, please contact the Head of IT and Information Compliance and Communications Officer.

6.2. If any College members are subjected to offensive or unacceptable behaviour in relation to social media, the incident should be reported to your Tutor (for students), or line manager (for staff).

6.3. Depending on the context of the incident, College members may wish to refer to the following policies:

6.3.1. For students – Discipline Policy (which incorporates harassment, bullying and discrimination)

6.3.2. For staff and Fellows – Dignity at Work Policy

6.4. Breaches which involve students, will be investigated with the relevant members of the Student Services Department, and may be escalated to the Dean of Discipline, in accordance with the College's Disciplinary Policy[4].

6.5. Breaches which involve staff will investigated with the HR Department, and dealt with in accordance with the relevant HR policies.

7. Policy Reviews

The Information Management Committee will review the Social Media Policy annually, or on an ad hoc basis when required, to ensure all legal and regulatory requirements are met. Wherever

[4] https://www.girton.cam.ac.uk/sites/default/files/2022-10/RevisedDisciplinePolicy-OCT22.pdf

necessary, stakeholders and College members will be consulted about changes to policies through the appropriate College committee or forum.

Last updated: 06 March 2024
Head of IT and Information Compliance

Version Control

Date	Version	Review Reason	Author
30/06/2020	Draft	New Policy review by IT Department	Head of IT and Information Compliance
15/11/2020	1.0	Publication	Head of IT and Information Compliance
01/02/2024	1.0	3-year review by IT Department	Head of IT and Information Compliance
14/06/2024	1.3	Publication	Head of IT and Information Compliance

Social Media Policy

Appendix A - Definitions

Staff

For clarity, the term staff means anyone working in any context for the College at any level or grade (whether permanent, fixed term or temporary) and including employees, retired but active members and staff, visiting Fellows, workers, trainees, interns, seconded staff, agency staff, agents, volunteers, and external members of College committees.

Members

Equally, the term member includes senior members (Fellows) and junior members (students and alumni) of the College when they are handling or processing personal information on behalf of the College, except when they are acting in a private or external capacity.