CITY OF GLASGOW COLLEGE

Social Media Policy

© 2014 City of Glasgow College

Charity Number: SCO 36198

Version: 1.0
06 AUG 2014
CONTROLLED VERSION ON CONNECTED

Lead Department: IT
Policy Lead: Executive Director, Infrastructure
Page 1 of 10

Table of Contents

Version: 1.0
06 AUG 2014
CONTROLLED VERSION ON CONNECTED

Lead Department: IT
Policy Lead: Executive Director, Infrastructure
Page 2 of 10

Social Media Policy

1. Introduction

1.1 City of Glasgow College encourages the safe and effective use of social media for all students and staff. Social media is generally regarded as the interaction between people using website and internet applications to create, share and exchange content, ideas and opinions. The rise in social media has resulted in fundamental changes in the ways individuals, groups and organisations communicate.

1.2 Social media is currently one of the most popular uses of the internet and has many benefits; it allows users to communicate easily and immediately with people they wouldn't otherwise be able to. However, there are also risks associated with social media which must be recognised and considered.

1.3 The classification of activity regarded as social media includes, but is not limited to:

- Social networking (e.g Facebook, LinkedIn)
- Blogs (e.g Twitter)
- Social photo and video sharing (e.g YouTube, Flickr)
- Collaborative projects (e.g Wikipedia, Wikia)
- Virtual social worlds (e.g Second Life)
- Virtual game worlds (e.g World of Warcraft)

Version: 1.0
06 AUG 2014
CONTROLLED VERSION ON CONNECTED

Lead Department: IT
Policy Lead: Executive Director, Infrastructure
Page 3 of 10

2. Purpose and Aims

This policy has been created to:

- Protect students and staff from the potential risks of social media use
- Provide guidance to students and staff using social media
- Set out the general principles that students and staff should adhere to when using social media, for their own safety and the safety of others

3. Scope

3.1 This policy is applicable to all students, teaching staff, support staff, Directors, and board members who may be using social media/ the internet to communicate:

- Content that identifies them as College employees or students
- Content relating to others within the College
- Content created in connection with their College employment or course
- Content about the College

For the purposes of this policy, the term '**user**' applies to any individual who satisfies these criteria.

3.2 This policy applies equally to the use of social media using either College-issued devices, or personal devices. College-issued devices include PCs, laptops, ipads, tablets and smartphones. The policy also applies equally to the use of social media on or off College premises. The location of the individual posting social media content does not matter. For example, unacceptable content uploaded from a home PC will be regarded in the same way as unacceptable content uploaded from a PC within the college.

3.3 This policy also applies to internal College IT systems which include a social networking aspect, such as MyCity's timeline and MyPortfolio groups.

3.4 Reasonable personal use of social media within scheduled breaks is permitted, as long as it does not interfere with work commitments and complies with this policy. Personal social media communications which do not, in any way, relate to the College are outwith the scope of this policy.

3.5 All other City of Glasgow College policies also apply in the context of social media.

Version: 1.0
06 AUG 2014
CONTROLLED VERSION ON CONNECTED

Lead Department: IT
Policy Lead: Executive Director, Infrastructure
Page 4 of 10

4. Policy Statement

. **4.1 Unacceptable content**

4.1.1 It is expected that users will act in a responsible and ethical manner when using social media, always treating others with dignity and respect. Regardless of the privacy settings applied to each site, users should assume that any content posted on social media is publically visible and permanent. Users should be aware that even if content is deleted, it may not be permanently removed. Each individual is personally liable and will be held accountable for the content that they post.

4.1.2 Unacceptable content includes, but is not limited to, content that is:

- Abusive
- Commercially sensitive
- Confidential
- Defamatory
- Discriminatory
- Fraudulent
- In violation of copyright laws
- Indecent
- Likely to be considered bullying or victimisation
- Likely to be considered harassment (related to protected characteristics)
- Likely to be considered offensive
- Likely to cause reputational damage
- Likely to identify an individual, without the permission of the individual
- Likely to promote violence or terrorism
- Malicious
- Misleading
- Obscene
- Offensive (for example, racially, religiously, sexually or politically)
- Pornographic
- Unlawful

4.1.3 Users must not attempt to access or use someone else's social media profile without their permission.

4.1.4 If users are found to be in breach of these guidelines, they may be subject to disciplinary action. Please see the relevant Disciplinary Policy for more information. In more serious cases, an individual may also be subject to civil or criminal legal proceedings. Social media must never be used in a way that breaches this or any other College Policy.

4.1.5 If student or staff users become aware that content of this nature has been posted by someone connected to the College, they should, respectively, make a Lecturer or Line Manager aware as soon as possible. If users wish to make a formal complaint about college-related social media, they should follow the normal Complaints Procedure.

Version: 1.0
06 AUG 2014
CONTROLLED VERSION ON CONNECTED
Lead Department: IT
Policy Lead: Executive Director, Infrastructure
Page 5 of 10

4.1.6 Permission from the Marketing department must be obtained before using College branding in any form of social media.

4.2 Personal safety

4.2.1 Students and staff should endeavour to keep themselves safe at all times when using social media. Information such as postal addresses, email addresses, telephone numbers and bank details should never be posted online. Users should also be wary of posting personal details, photographs or details of their current location on social media sites.

4.2.2 Unwanted contact can be made very easily via social media sites; users should be aware of this and not accept befriending invitations from strangers.

4.2.3 If using a shared device, users should ensure that they are logged off of all social media sites before shutting down the device.

4.3 Online bullying, harassment and victimisation

4.3.1 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 through social media, they should carry out the following steps:

- Do not respond directly to the comments
- Retain evidence
- Report the situation immediately to a Curriculum Head or Line Manager

4.3.2 Students: Full definitions of bullying, harassment and victimisation can be found in the Student Bullying and Harassment Policy. Any examples of these behaviours taking place through social media will be dealt with through the Student Disciplinary Procedure.

4.3.3 Staff: Please refer to the Dignity at Work Policy. Any examples of these behaviours taking place through social media will be dealt with through the College's Disciplinary Policy and procedures.

4.4 Monitoring and Privacy

4.4.1 Users should be aware that the College reserves the right to monitor and review all aspects of use of the College IT network 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.

Version: 1.0
06 AUG 2014
CONTROLLED VERSION ON CONNECTED

Lead Department: IT
Policy Lead: Executive Director, Infrastructure
Page 6 of 10

4.4.2 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 Police or Security Services, as allowed by current legislation
- Requests made under the Data Protection Act (1998) or Freedom of Information Act 2000 (Scotland 2002)
- Requests to establish facts as part of a misconduct investigation
- Requests from the employee themselves
- To facilitate the operation, repair and essential maintenance of College systems

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

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

4.5 Relationships between staff and students online

4.5.1 Where possible, the preferred method of online communication between staff and students is the Virtual Learning Environment, MyCity, or College email. Teaching staff should use MyCity when publishing course resources and materials.

4.5.2 However, the College accepts that social media can be a useful way for staff and students to communicate and may, in some circumstances, be beneficial to the learning and teaching process. The College has a responsibility for the welfare of all students and staff, which extends to social media activity. If staff choose to use external social media platforms as an alternative/ supplementary tool for learning and teaching, professional and personal boundaries must be fully recognised and respected.

4.5.3 Staff and students must not make or accept invitations to be friends, or form similar connections on social media sites, unless there is a legitimate College business reason to do so. Staff should be wary of befriending students on social media sites and must at all times observe the boundaries of the professional staff/student relationship. It is strongly recommended that members of staff create separate professional and personal social networking profiles if using social media in this way.

4.6 College-maintained social media sites

4.6.1 The College maintains official accounts for social media sites such as Facebook, Twitter and Flickr, links to which can be found via the College website. These sites are monitored by the College Marketing department and are the preferred accounts for users to communicate and interact with City of Glasgow

Version: 1.0
06 AUG 2014
CONTROLLED VERSION ON CONNECTED

Lead Department: IT
Policy Lead: Executive Director, Infrastructure
Page 7 of 10

College.

4.6.2 Responsibility for the suitability of information posted on College-maintained social media sites lies 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. The College will remove any content found to be inappropriate and may block users from posting on these sites if it becomes necessary.

4.6.3 If users become aware of inappropriate material being posted outwith normal working hours, they should report this to the site provider. Users should familiarise themselves with the Terms and Conditions of any social media site they are using.

4.6.4 If staff or students 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 Head of Marketing. If the social media profile is affiliated with a specific course, the user must also obtain permission from the relevant Curriculum Head.

4.7 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 should be referred to the Marketing department or a Line Manager.

5. Legislation

5.1 All social media use must comply with existing UK legislation and EU directives.

5.2 The main laws covering use/misuse of social media are:

- Anti-Terrorism, Crime and Security Act 2001
- Copyright, Designs and Patents Act 1988
- Data Protection Act 1998
- Equality Act 2010
- Freedom of Information (Scotland) Act 2002
- Human Rights Act 1998
- Malicious Communications Act 1988
- Offences (Aggravation by Prejudice) (Scotland) Act 2009
- Regulation of Investigatory Powers Act (RIPA) 2000

Version: 1.0
06 AUG 2014
CONTROLLED VERSION ON CONNECTED
Lead Department: IT
Policy Lead: Executive Director, Infrastructure
Page 8 of 10

6.References

6.1 Policy Framework

Associated Policies and Procedures	Title
Policy	IT Acceptable Use
Policy	Data Protection (for Staff and Students)
Policy and Procedure	Disciplinary
Procedure	Complaints Handling
Policy	Diversity and Equalities
Policy	Personal Relationships Between Staff and Students
Policy	Safeguarding
Policy	Student Bullying and Harassment
Policy (Draft)	Dignity at Work

6.2 Other College Policies and Procedures

Policy / Procedure	Title
	Staff Code of Conduct
Policy and Procedure	Grievance
Policy (Draft)	Bring Your Own Device (BYOD)
Policy (Draft)	Information Security

Version: 1.0
06 AUG 2014
CONTROLLED VERSION ON CONNECTED

Lead Department: IT
Policy Lead: Executive Director, Infrastructure
Page 9 of 10

7. Document Control and Review

Approval Status	Approved
Approved by	Students, Staff and Equalities Committee
Date Approved	6 August 2014
EQIA Status	EQIA Conducted? Yes: ☒ No: ☐
Proposed Review Date	2017
Lead Department	Infrastructure
Lead Officer(s)	Executive Director, Infrastructure
Board Committee	Students, Staff and Equalities Committee
Copyright © 2012 City of Glasgow College	Permission granted to reproduce for personal use only. Commercial copying, hiring lending, posting online is strictly prohibited

8. Revision Log

Version Date	Section of Document	Description of Revision
Version 1 06 Aug 2014	All	First Version of City of Glasgow College Social Media Policy

Version: 1.0
06 AUG 2014
CONTROLLED VERSION ON CONNECTED

Lead Department: IT
Policy Lead: Executive Director, Infrastructure
Page 10 of 10