Social Media Policy

UNCONTROLLED WHEN PRI

November 2013

Also available in large print (16pt)
And electronic format.

Ask Student Services for details.

www.perth.ac.uk

Perth College is a registered Scottish charity, number SC021209

University of the Highlands and Islands
Perth College

Version Control History

Version Number	Date of Change	Summary of Revisions Made
0		
1	August 2016	Footer updated to reflect new template model
1.2	January 2019	• New section to cover GDPR requirements. • All social media accounts must be approved by the Marketing Team Leader. • Once, approved all social media accounts must be set up by the marketing team. This will reduce risk and ensure all accounts are correctly set up, on brand and that the managers of those accounts are equipped with the necessary skills to manage them effectively.
1.3	June 2019	• Re procedure for retrospective approval of existing accounts - active existing accounts have been evaluated as appropriate for business needs and may continue to operate.

UNCONTROLLED WHEN PRINTED

Social Media Policy

1 Purpose

The purpose of this policy is as follows:

- To encourage good practice.
- To protect Perth College UHI, its staff and students.
- To clarify where and how existing policies and guidelines apply to social media.
- To promote effective and innovative use of social media as part of the College's activities.

The growth in social media, particularly social networking sites, has created increased opportunity for media communications that have an impact upon the reputation of the College.

The term 'social media' is used to describe dynamic and socially-interactive, networked information and communication technologies, for example, YouTube, Flickr and social networking sites such as Facebook, Twitter and Instagram.

2 Scope

All staff and students that use social media tools to communicate internally or externally for communications on behalf of the college, research or any other College business.

The use of social media by all staff and students is subject to College policy governing employee and student conduct. These policies are listed at Section 8.

3 Definitions

3.1 Corporate and Authorised Users

Any member of staff, or department, who is authorised to communicate with third parties, the public, or students via social media tools. Authorisation is normally by the manager of the relevant service.

3.2 Institutional Tools

Organisational tools which can often perform the same function as social media tools, but are within local control, usually that of University of the Highlands and Islands. For further details, see Appendix 1.

UNCONTROLLED WHEN PRINTED

For the purposes of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes online social forums such as Twitter, Facebook, Instagram and LinkedIn. Social media also covers blogs and video, and image-sharing websites such as YouTube.

Employees should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area. Employees should follow these guidelines in relation to any social media that they use.

3.3 Personal Data

In this document, personal data is defined as data, including photographs, video or audio recordings which is gathered with consent for marketing purposes.

3.4 Interactive Platforms

Online tools which allow for a more interactive experience, in the form of blogs, wikis, forums, etc.

4 Key Principles: Use of Social Media

4.1 Employees should not spend an excessive amount of time while at work using social media websites, even if it is as part of their work, with the exception of marketing. This is likely to have a detrimental effect on employees' productivity. They should ensure that use of social media does not interfere with their other duties.

4.2 The organisation reserves the right to monitor employees' internet usage, but will endeavour to inform an affected employee when this is to happen and the reasons for it. The organisation considers that valid reasons for checking an employee's internet usage include suspicions that the employee has:

- Been spending an excessive amount of time using social media websites for non-work-related activity;
- Acted in a way that is in breach of the rules set out in this policy or other college policies and procedures.

4.3 There should be no systematic or routine checking of employees' online social media activities.

4.4 Set your privacy settings to control who can, and cannot, view your personal information and content. Tight privacy settings may limit dissemination of your information directly, but those with legitimate access can still share with a wider audience.

UNCONTROLLED WHEN PRINTED

4.5 Information, images and video available on social media sites may influence your professional reputation with current and potential future employers.

4.6 Any inappropriate activity brought to the College's attention which, is deemed to be unprofessional or to bring the College into disrepute, will be dealt with under the relevant College procedures.

4.7 Do not post anything that you would not share in any public forum. In particular, do not discuss a situation involving named or pictured individuals on a social media site without their knowledge or permission. You should be aware of protecting not only your own privacy, but also the privacy of others.

4.8 In all situations, you should take advance steps to ensure that material you post to authorised social media accounts at the College does not contain material that reflects negatively on the College or members of the College community.

4.9 The College may refer to social networking sites when investigating breaches of college rules, eg cheating, harassment, anti-social behaviour. Further information on student and staff disciplinary procedures can be found on the College website.

4.10 Employees are allowed to make reasonable and appropriate use of social media websites from the organisation's computers or devices, provided that this does not interfere with their duties.

4.11 Employees are allowed to access social media websites from the organisation's or their own computers or devices at certain times. Employees must limit their use of social media to their official rest breaks such as their lunch break/times as agreed by their manager when not using it for work-related purposes.

4.12 The organisation has specifically blocked use of ask.fm. Access to other social media websites may be withdrawn in any case of misuse.

4.13 The organisation encourages employees to make reasonable and appropriate use of social media websites as part of their work. It is an important part of how the organisation communicates with its stakeholders, promotes its services, and the learning and teaching process. Staff should refer to the E Safety Policy, section 4.4 with regard to communication with students online, and how the process should be managed in a professional manner.

4.14 Approved employees may contribute to the organisation's social media activities, for example by writing for our blogs, managing a Facebook account, running an official Twitter account for an organisational department.

UNCONTROLLED WHEN PRINTED

4.15 All organisational accounts must be set up by the Marketing Team. Approval must be granted from the line manager and Marketing Team Leader before an account can be sent up. All passwords must be shared with the Marketing Team Leader.

Active existing accounts have been evaluated as appropriate for business needs and may continue to operate.

4.16 A social media notification form is to be completed in order to gain permission to use social media tools for organisational or learning and teaching purposes. The form is available at Appendix 2.

4.17 Employees should be rightly proud of working for the College, which recognises that it is natural for its staff sometimes to want to discuss their work on social media. However, the employee's online profile (for example, the name of a blog or a Twitter name) must not contain the organisation's name.

4.18 If employees do discuss their work on social media (for example, giving opinions on their specialism or the sector in which the organisation operates), they must include on their profile a statement along the following lines: "The views I express here are mine alone and do not necessarily reflect the views of my employer."

4.19 Any communications that employees make in a personal capacity through social media must not:

- Bring the organisation into disrepute, for example by:
    - Criticising or arguing with customers, colleagues or rivals;
    - Making defamatory comments about individuals, the college or other organisations or groups;
    - Posting images that are inappropriate or links to inappropriate content.
- Breach confidentiality, for example by:
    - Revealing trade secrets or information owned by the organisation;
    - Giving away confidential information about an individual (such as a colleague or customer contact) or organisation (such as a rival business);
    - Discussing the organisation's internal workings (such as deals that it is doing with a customer/or client, or its future business plans that have not been communicated to the public).
- Breach copyright, for example by:
    - Using someone else's images or written content without permission;
    - Failing to give acknowledgement where permission has been given to reproduce something.

UNCONTROLLED WHEN PRINTED

- Do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
  - 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 bully another individual (such as an employee of the organisation);
  - Posting images that are discriminatory or offensive (or links to such content).

5 Responsibilities

5.1 The Marketing Team Leader is the owner and author of this policy.

5.2 College managers have a responsibility to assess, approve and monitor use of social media within their areas of line management. (See Appendix 2)

5.3 All College staff have a responsibility not to post any materials on social media websites that may bring the College into disrepute.

5.4 Employees must be aware at all times that, while contributing to the organisation's social media activities, they are representing the organisation. Staff who use social media as part of their job must adhere to the following rules:

- Employees should use the same safeguards as they would with any other form of communication about the organisation in the public sphere. Be aware of the E-Safety policy, and the rules regarding 'friending' students on social network sites.
- Ensure that the communication has a purpose and a benefit for the organisation.
- Obtain permission from a manager and the Marketing Team Leader before embarking on a public campaign using social media; and, where appropriate, getting a colleague to check the content before it is published.

6 Use of Social Media in the Recruitment Process

Unless it is in relation to finding candidates (for example, if an individual has put his/her details on social media websites for the purpose of attracting prospective employers), the HR department and managers should conduct searches, either themselves or through a third party, on social media only when these are directly relevant to the applicant's skills or claims that he/she has made in the recruitment process. For instance:

- A prospective employee might claim that he/she has used social media in his/her previous job (for example, as a publicity tool) and provide the link;

UNCONTROLLED WHEN PRINTED

- A prospective employee's social media use may be directly relevant to a claim made in his/her application (for example, if he/she runs a blog based around a hobby mentioned in his/her CV or a skill in which he/she claims to be proficient).

There shall be no systematic or routine checking of prospective employees' online social media activities, as conducting these searches during the selection process might lead to a presumption that an applicant's protected characteristics (for example, sexual orientation or religious beliefs) played a part in a recruitment decision. This is in line with the organisation's equal opportunities policy.

Quality approval check of the policy is the responsibility of the Quality Manager who will arrange for the policy to be posted on the intranet or the College website.

7 Social Media and GDPR (General Data Protection Regulation)

7.1 All corporate social media managers must:

- Complete all GDPR mandatory training before being granted account access.
- Ensure they complete the relevant photography and videography consent forms. These are available on PerthNet here: http://www.perthnet.uhi.ac.uk/crosscollegeteams/marketing/Pages/default.aspx
- Store all forms in a secure location, for example in a locked cabinet.
- Store all personal data, including photos and videos, in an encrypted and secure location.
- Securely destroy all personal data within 4 years of gathering it.
- Alert the Marketing Team Leader to any requests to revoke an individual's consent for personal data to be destroyed and removed from marketing channels. All personal data pertaining to that individual must then be deleted with immediate effect.

UNCONTROLLED WHEN PRINTED

8 Linked Policies/Related Documents

Data Protection Policy

Dignity in the College Anti Bullying and Harassment Policy

Staff and Student Disciplinary Procedures

E-Safety Policy

ICT Acceptable Use Policy for Staff and Students

ICT Security Policy

Safeguarding Policy and Procedure Protecting Children Young People Adults at Risk and Staff

Student Charter

UNCONTROLLED WHEN PRINTED

Appendix 1: Institutional Tools

The College recommends the use of institutional tools where these have been designed to allow for materials delivery, file sharing, communication and assessment.

Blackboard VLE

The institutional VLE provides an online tool to support learning and teaching. Blackboard offers a range of course and communication features, including content management, and tools such as; discussion boards, chat forums, blogs, wikis, journals, mashups, etc. Blackboard is an ideal tool for administering online coursework submission via the Grade Centre, which is secure, private and designed to make administration of submitted materials as efficient as possible.

Access the VLE here: **https://www.blackboard.uhi.ac.uk**

myUHI

The myUHI Citrix service provides a virtual UHI desktop on any internet connected computer. You can log into the service and access your files from any computer and you can also access a range of software applications that run across the internet – this means that you don't have to have these applications on your computer but you can still use them from any computer connected to the internet. myUHI requires you to log into the service using your UHI user name and password.

https://my.uhi.ac.uk/http/m2-wisg2.uhi.ad.local/Citrix/XenApp/auth/login.aspx

Office 365

The institutional email client is Microsoft Office 365 (using Outlook client).

Login here: **http://outlook.com/uhi.ac.uk**

Contact the IT department to setup a local Outlook client for your PC.

UHI Dropbox

UHI Dropbox allows you to share files larger than 25Mb (the Outlook file size limit).

Access the Dropbox here: **http://dropbox.uhi.ac.uk/index.php?action=login**

UNCONTROLLED WHEN PRINTED

UHI Mahara

UHI Mahara is a fully featured electronic portfolio system with social networking features to create online learning communities.

Login here: **http://uhi-mahara.co.uk/**

Training and familiarisation tools are available when you login, using your normal institutional ID and password.

UHI Toolkit

An online service to facilitate the sharing of resources by staff across the University of the Highlands and Islands. Use your institutional ID and password to login, search and browse.

http://www.toolkit.uhi.ac.uk/?locale=en

UNCONTROLLED WHEN PRINTED

Appendix 2: Social Media Notification Form

This form should be completed and submitted to your line manager in order to apply for access to use social media sites for college related business. Your request will be reviewed by your line manager and the Marketing Team Leader.

Name:

Department:

Aims and Objectives

Why do you consider social media as a key communication element for your work?

What are your key objectives for the use of social media?

What will the use of social media add to the service you offer?

Who will be your intended audience?

Do you have a preference for which tool you will use?

Facebook ☐ Twitter ☐ YouTube ☐

Instagram ☐

Other:

How will you measure success for social media use?

Are there any potential risks in the use of social media?

How will you address those risks?

Who will moderate the social media site and content?

Approved by: Date:

A copy of this completed form should be sent to Lisa Findlay in the Marketing Department.

UNCONTROLLED WHEN PRINTED