UHI PERTH

Digital Etiquette Policy

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.
1.4	December 2020	• Policy is to be wider to include all digital online communications
1.5	June 2022	• Policy reviewed in light of changing hybrid working patterns and impact on digital social behaviour. • Title Change from Social Media Policy to Digital Etiquette Policy
1.6	March 2023	• Rebranded

Digital Etiquette Policy

1   Purpose

The purpose of this policy is as follows:

- To encourage good 'netiquette' practice and establish the parameters of acceptable behaviour whilst using online communication platforms, including learning and teaching tools, and video conferencing platforms such as Webex and MS Teams. To protect Perth College UHI, its staff and students.
- To clarify where and how existing policies and guidelines apply to online communications
- To promote effective and innovative use of social media and other digital platforms as part of the College's activities

The growth in online digital platforms, has created increased opportunity for media communications that have an impact upon the reputation of the College.

'Netiquette' means online etiquette and encapsulates behaviour, customs, manners, politeness and social norms.

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

Online digital communication platforms include video meetings, learning and teaching tools, blogs, and chatrooms. These may be open or closed group access.

2   Scope

All staff and students that use online communication tools to communicate on and off campus related to college business or studies.

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 public online communication 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.

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

3.3 Personal Data

In this document, personal data is defined as data, including photographs, video or audio recordings, which if used for promotional reasons, must be 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.

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

Title: Digital Etiquette Policy   **Owner:** Vice Principal, External Engagement
Version/Status: V1.6/Draft   **Lead Author:**
Approved By/Date: CMT, November 2013   **Lead Editor:** Marketing Team Leader
Issue Date: March 2023   **EQIA Approval Date:**

QUAL/080   2 of 9   **Perth College**

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   To safeguard the privacy of users and viewers (GDPR), 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, or brings into disrepute the College, UHI or members of the College community.

4.9   The College may refer to social networking sites when investigating breaches of 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, supporting LinkedIn content, managing a Facebook account, or running an official Instagram or Twitter account for an organisational department.

Title: Digital Etiquette Policy
Version/Status: V1.6/Draft
Approved By/Date: CMT, November 2013
Issue Date: March 2023

Owner: Vice Principal, External Engagement
Lead Author:
Lead Editor: Marketing Team Leader
EQIA Approval Date:

QUAL/080   3 of 9   **Perth College**

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.

Any accounts that have not been set up in this way but promote the college and its activities must be evaluated by the Marketing Team Leader as appropriate for business needs, negating business and reputational risk. Permission may or may not be given to operate.

4.16   A meeting with the Marketing Team must be made in order to gain permission to use social media tools for organisational or learning and teaching purposes. Please contact pc.marketing@uhi.ac.uk to discuss before setting up an account.

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." However, the use of such a disclaimer is not sufficient disclaimer to stop the enforcement of disciplinary action should it be deemed that behaviour is outwith the expectations of behaviour outlined by the key principles of this policy.

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 secrets or information owned by the College or UHI;
    - Giving away confidential information about an individual (such as a colleague or student) or organisation (such as a partner business);
    - Discussing the organisation's confidential internal workings

Title: Digital Etiquette Policy   **Owner:** Vice Principal, External Engagement
Version/Status: V1.6/Draft   **Lead Author:**
Approved By/Date: CMT, November 2013   **Lead Editor:** Marketing Team Leader
Issue Date: March 2023   **EQIA Approval Date:**

QUAL/080   4 of 9   **Perth College**

- 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.

- 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   Key Principles: Use of Online Digital Platforms

- Reflect the essence of this Digital Etiquette Policy, but specifically noting expectations while using video conferencing and learning and teaching tools.
- To protect users from damaging behaviour and naïve use
- To ensure there is no intention to cause behaviour that is deemed inappropriate or illegal
- Staff and students should be aware of netiquette norms when using digital communications, particularly when remote and online learning.
- These expectations include:
  - Be aware of strong language, all caps, and exclamation points, this can seem rude.
  - Avoid sarcasm and humour, it doesn't always come across as intended online.

  - Please make best use of proper punctuation, spelling and grammar.
  - Be kind and respectful, keep in mind the feelings and opinions of others.
  - What you share in an online classroom is part of a permanent digital record.
  - In a video conference scenario, remember you are on camera, be aware of your surroundings and stay engaged, muting your microphone when you are not speaking for the comfort of other participants.

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.

5.3   All College staff have a responsibility not to post any materials on digital online communications that may bring the College into disrepute.

Title: Digital Etiquette Policy   **Owner:** Vice Principal, External Engagement
Version/Status: V1.6/Draft   **Lead Author**:
Approved By/Date: CMT, November 2013   **Lead Editor:** Marketing Team Leader
Issue Date: March 2023   **EQIA Approval Date:**

QUAL/080   5 of 9   **Perth College**

5.4   Employees must be aware at all times that, while contributing content and discussions on behalf of the organisation's digital communication activities, they are representing the organisation. Staff who use digital communications 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 'befriending' 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;
- 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 Social Media managers must:

- Complete all GDPR mandatory training before being granted account access.

Title: Digital Etiquette Policy
Version/Status: V1.6/Draft
Approved By/Date: CMT, November 2013
Issue Date: March 2023

Owner: Vice Principal, External Engagement
Lead Author:
Lead Editor: Marketing Team Leader
EQIA Approval Date:

QUAL/080   6 of 9   **Perth College**

- Ensure they complete the relevant photography and videography consent forms. These are available on PerthHUB.
- Store all forms in a secure location, for example in a locked cabinet.
- Store all personal data, including photos and videos, in a 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.

8   Linked Policies/Related Documents

Data Protection Policy and Guidance

Dignity in the College Anti Bullying and Harassment Policy and Procedure

GDPR Subject Access Request Procedure

Staff and Student Disciplinary Procedures

E-Safety Policy

Equality, Diversity and Inclusivity Policy

Promoting a Positive Learning Environment 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

Title: Digital Etiquette Policy
Version/Status: V1.6/Draft
Approved By/Date: CMT, November 2013
Issue Date: March 2023
Owner: Vice Principal, External Engagement
Lead Author:
Lead Editor: Marketing Team Leader
EQIA Approval Date:

QUAL/080   7 of 9   **Perth College**

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.

PerthHUB, our internal Intranet.

myday
The myday service provides a virtual desktop service on any internet connected computer tro allow to access all your digital tools. You need to log in using your UHI username and password.
https://myday.uhi.ac.uk/dashboard/students

Brightspace VLE
The institutional Virtual Learning Environment (VLE) provides an online tool to support learning and teaching. Brightspace offers a range of course and communication features, including content management, and tools such as; discussion boards, chat forums, blogs, wikis, journals, mashups, etc. This is an ideal tool for administering online coursework submission, which is secure, private and designed to make administration of submitted materials as efficient as possible.
https://brightspace.uhi.ac.uk/

Office 365
The institutional email uses Microsoft Office 365
https://www.uhi.ac.uk/en/lis/email/

UHI Dropbox
UHI Dropbox allows you to share large files.
UHI Dropbox

UHI Mahara
UHI Mahara is a fully featured electronic portfolio system with social networking features to create online learning communities. Training and familiarisation tools are available when you login, using your normal institutional ID and password.
Home - Mahara (uhi.ac.uk)

UHI Toolkit
The UHI Toolkit is a database of learning resources that is maintained by the Educational Development Unit.

Title: Digital Etiquette Policy   **Owner:** Vice Principal, External Engagement
Version/Status: V1.6/Draft   **Lead Author**:
Approved By/Date: CMT, November 2013   **Lead Editor:** Marketing Team Leader
Issue Date: March 2023   **EQIA Approval Date:**

QUAL/080   8 of 9   **Perth College**

Title: Digital Etiquette Policy
Version/Status: V1.6/Draft
Approved By/Date: CMT, November 2013
Issue Date: March 2023

Owner: Vice Principal, External Engagement
Lead Author:
Lead Editor: Marketing Team Leader
EQIA Approval Date:

QUAL/080   9 of 9   **Perth College**