STAFF/STUDENTS

SOCIAL MEDIA & NETWORKING POLICY INCLUDING ONLINE COMMUNICATIONS AND PERSONAL INTERNET PRESENCE

The College seeks to ensure through our functions, policies and employment practices that we do not discriminate on any grounds and that the College acts in accordance with its statutory obligations under the equality duties and in compliance with current legislation.

This policy is to be read and applied in conjunction with the following:

- *The College STAFF Code of Conduct Policy*
- *The College STAFF Disciplinary Procedure*
- *The College STUDENT Disciplinary Procedures*
- *The College STAFF Harassment and Bullying Policy and Procedure*
- *The College STAFF/STUDENT/GOVERNOR Single Equality Scheme*
- *The College STAFF/STUDENT Safeguarding Policy*
- *The College Preventing Extremism and Radicalisation Policy*

For further information and guidance contact the College's designated Senior Member of Staff with lead responsibility for safeguarding:

Kathryn Caulfield (Head of Student Services; Designated Safeguarding Lead

1. INTRODUCTION

1.1. The College acknowledges that staff and students have a right to freedom of expression and recognises that they are participating widely in social media and other internet based communication and networking sites.

1.2. The College acknowledges that staff and students may also build an online presence through the creation of personal websites, blogs and other channels.

1.3. This document offers guidance in the use of online technologies including, but not limited to: social media and networking, photo sharing, video sharing, virtual worlds, wikis, blogging, forums and personal websites.

1.4. Whilst there are many benefits to using such technology, this document offers guidance on how the College expects staff and students to conduct themselves in a safe and appropriate way to minimise the risks of misinformation, inappropriate communication, unprofessional behaviour, bullying and harassment or other negative impacts on the reputation of the College or employees.

1.5. This document offers guidance on the safe use of the internet and how to protect your personal information.

2. GENERAL GUIDANCE FOR STUDENTS

2.1. Students must assume that everything they post or upload to the internet is permanent and subject to being public, even if that information has been deleted or removed. Students must take responsibility for what they write, post or distribute online.

2.2. Students should be aware of who can view their online content and always use the appropriate privacy settings to protect information they do not wish others to view.

2.3. Students are reminded that all content they post, upload or publish on social networking or other internet sites that is not protected by security or privacy settings may be viewed, read or downloaded by the College, university admissions staff, future employers and any other persons with internet access.

2.4. The College may take disciplinary action against any student that personally posts, uploads or publishes any content that the College deems abusive, defamatory or unsubstantiated about the College, its employees, students, parents, governors, exam boards or any other persons connected professionally to the College.

2.5. The College will take immediate and firm action when made aware of any case of online bullying, harassment or abuse made by a student towards another student, staff member or any other person within the College community.

2.6. The College may take action in line with the "Preventing Extremism and Radicalisation Policy" when made aware of any content published or viewed by students promoting extremist actions, views, images or materials

2.7. Students are reminded to be respectful of others when posting opinions, comments or other content online and to follow the College policies including Code of Conduct, Equality and Diversity and Safeguarding.

2.8. Students must obtain permission before uploading personal details, photographs or video content of other students and staff members to social networks or other internet sites.

2.9. The College strongly advises students against inviting a staff member to join, follow or become part of any personal network, profile, page or other channel.

2.10. The College will offer guidance, advice and support to its students on the safe use of social networks and other internet sites.

3. GUIDANCE ON THE SAFE USE OF THE INTERNET

3.1. Avoid posting any personal or financial details online.

3.2. Be aware of who can see what you are posting online. Your online content could be accessed by College staff, students, future employers or university admissions staff, unless secured.

3.3. Use privacy settings, where available, to protect your personal information.

3.4. Change your usernames and/or passwords regularly and include capital letters, numbers or symbols to make them more secure.

3.5. Consider a second email account for use in more formal communication (e.g. a future employer may find addresses such as 'fluffypinkbunny2013@hotmail.com' unprofessional)

3.6. Chat rooms, social networking sites and other internet sites should be used with care. Remember the person you are talking to may not be being honest about who they are, their age or any other aspect of their profile and identity.

3.7. Do not disclose information that could be used inappropriately e.g. giving holiday dates could indicate when your house is empty and lead to burglary.

3.8. Report any contact that is made with you via the internet that is inappropriate, abusive or that threatens your safety in any way (see section 8).

3.9. Beware of online scams, especially financial ones, and do not disclose financial or account information or PIN numbers online or via email.

3.10. Only make online purchases from reputable sites using secured pages for financial transactions (often indicated by the prefix https://).

3.11. Bullying online is unacceptable and will lead to disciplinary action. Do not post unkind, abusive or threatening messages or images of anyone, including students, staff or other members of the College community.

4. BULLYING AND HARASSMENT

If an individual receives communication(s) that they perceive to be bullying or harassing them, the College advises that they:

4.1. Avoid responding to the communication(s).
4.2. Keep electronic and printed copies of the communication(s).
4.3. Unfriend/unfollow and block the account(s) from which communication(s) are being sent.
4.4. Report the account(s) and the communication(s) to the website via their online form.
4.5. Make your parents/guardians aware of the issues and discuss it with them. In certain cases it may be necessary to involve the College and also the Police.
4.6. If preferable or easier make a member of staff at the College aware of the issue and discuss it with them.

5. GENERAL GUIDANCE FOR STAFF

5.1. Staff are reminded that their professional responsibilities at the College require them to act with care and professionalism when posting information, images or other material on the internet, especially when making reference to their employment at the College.
5.2. Staff must assume that everything they post or upload to the internet is permanent and subject to being public, even if that information has been deleted or removed. Staff must take responsibility for what they write, post or distribute online.
5.3. Staff should be aware of who can view their online content and always use the appropriate privacy settings to protect information they do not wish others to view.
5.4. Staff should be aware that their online content may be shared/forwarded/reposted/retweeted by others, outside of the original and intended security settings.
5.5. Staff must always strive to create a clear distinction between their personal and professional lives.
5.6. Staff must be aware that seemingly innocent information, photographs, videos, opinions or comments are vulnerable to misrepresentation, misinterpretation and unauthorised distribution via the internet.
5.7. Staff should at all times behave with integrity and ensure that their online presence is professional.

6. STAFF-TO-STUDENT ONLINE CONTACT AND COMMUNICATION

6.1. Staff must always ensure any online contact with students is within the boundaries of their professional responsibilities at the College.
6.2. All online communications between staff and students should only ever take place for legitimate and professional reasons.
6.3. All staff-to-student online interactions should be meaningful and professional.
6.4. Staff are expected to use the internet positively for communication, collaboration and learning.
6.5. Write appropriately for your expected audience and promote productive communication. Be personable, add value and encourage responses.
6.6. If a situation arises of a legitimate yet non-professional reason for online communication or association to take place (e.g. common membership of a club, society, team or organisation outside College) staff must be aware of the risks involved and must seek to limit those risks.
6.7. The College strongly advises staff against inviting a student or parent/guardian to join, follow or become part of a personal network or profile where there is no professional or educational justification for doing so.

6.8. The College strongly advises staff against accepting an invitation from a student or parent/guardian to join, follow or become part of a student personal network or profile where there is no professional or educational justification for doing so.

6.9. The College recommends a minimum of 3 years have elapsed before staff consider accepting invitations to join, follow or become part of a personal network or profile from former students.

6.10. The College strongly advises staff to protect all personal profiles, photographs, videos or other information by using any available security or privacy settings, and to consider the creation and use of a 'professional' profile when in contact with students.

6.11. Staff should only use the College email system for any email contact with students. Staff who use personal email for official college communications are in violation of the policies of the Henley College.

6.12. If a staff member is unsure or concerned about any aspect of their online communication or association with students they must seek advice from their Head of School/Section, the Director of HR and Professional Development or Designated Safeguarding Officer.

6.13. Staff should only use College recording equipment for taking photos, videos or any other types of recordings of students. Personal devices should not be used.

6.14. The College prohibits staff from giving students personal contact details such as mobile phone numbers or personal email addresses.

7. COLLEGE REPUTATION AND BRAND

7.1. Do not post, upload or distribute any material that may damage your own or the College's reputation, or that of other staff members/students.

7.2. Do not post, upload or distribute personal details or photographs of other staff members/students without their permission.

7.3. Do not post, upload or distribute any confidential or business sensitive information.

7.4. Do not post, upload or distribute comments, views or information that may be abusive, defamatory or unsubstantiated about the College, its employees, students, parents, governors, exam boards or any other persons connected professionally to the College.

7.5. Respect College policy guidelines and other codes of practice.

7.6. Do not use the College logo on personal web pages or other unendorsed products or sites.

7.7. Clearly identify and indicate when you are not speaking officially for the College by using a disclaimer such as "the views contained in these web pages are my personal views and do not represent the views of The Henley College".

7.8. Always seek to use the College email system for all email contact with other employees, students, parents, governors, exam boards or any other persons connected to the College.

8. MONITORING, REPORTING AND MANAGEMENT

8.1. The College reserves the right to view any public content on the internet that has been posted or uploaded by staff and students.

8.2. The College reserves the right to act upon any online content submitted personally by staff or students that the College deems abusive, defamatory or unsubstantiated about the College, its employees, students, parents, governors, exam boards or any other persons connected professionally to the College.

8.3. Staff are obliged to report any online content submitted personally by staff or students that could be considered abusive, defamatory or unsubstantiated about the College, its employees, students, parents, governors, exam boards or any other persons connected professionally to the College.

8.4. Where staff or students are the subject/target of groups, pages, sites or posts over which they have no control, the College will always try to help protect individuals and their reputations along with the reputation of the College.

8.5. The College is fully committed to Safeguarding all staff and students at the College, and will always take immediate and appropriate action when made aware of any cases of online bullying,

harassment, abuse or other inappropriate content about staff or students in line with the College's policies and codes of practice.

8.6. The College may monitor, and share with external agencies when requested, details of any individual believed to be viewing or sharing extremist views, actions or images, or materials related to radicalisation

8.7. The College will offer guidance to staff and students on the benefits and risks of having an online presence and on how to use the Internet safely.

8.8. The College reserves the right to remove any content it deems unsuitable from any groups, pages, sites or posts over which it has control.

8.9. The College reserves the right to refuse the use of any College owned logos, images or text on any other groups, pages or sites.

Social media and networking policy
Author: Head of Marketing and Admissions (DLAM): April 2014
Reviewed: Head of Student Services; Designated Safeguarding Person (CECK): Oct 2014
Amended: Head of Student Services; Designated Safeguarding Person (CECK): Dec 2014
Reviewed and Amended: IT & Systems Manager: Feb 2016
Reviewed July 2018