

## SOCIAL MEDIA AND E-SAFETY POLICY

### Background

The internet and Social Networking revolution have created new and instantaneous channels for information sharing and communication which are freely available and accessible to all. For the College this can and does offer huge advantages in terms of our ability to communicate with students. For students, there are considerable benefits to both their learning and their social experience at college. However, such apparently informal and instant communication can reach a very wide audience and is permanent, increasing the risk of misinformation, inappropriate communication, unprofessional behaviour and negative impact.

The idea of a static, moderated website bears little relation to the modern internet where most sites are made up of content from numerous sources and without a clearly defined 'author'. There are a significant number of websites which give opportunities for users to contribute content.

### 1. What are the advantages of using social media in colleges:

The AOC Social Media task group identified the advantages of using social media in colleges as:

- Ignore it at your peril – it's out there!
- Marketing, communications, retention, achievement
- Student experience
- Popular culture, student language
- Good way of measuring Return on Investment
- Improves Google ratings
- Great starting point for VLEs; curriculum delivery and development
- Opens up wider opportunities – great training vehicle for staff
- Instant communication of messages to narrow or broad audiences
- Customer service vehicle: versatile reputation tool

### 2. General Principles

The College recognises that staff and students have lives outside college and can and will make decisions about their own use of social networking sites. To inform these decisions, and for the protection of both staff and students, this policy is designed to be clear and explicit about appropriate behaviour in the use of social media and electronic communication and the College's responsibility to its staff and students to promote e-safety.

We take the view that **all** Information posted on websites should be considered as **published, permanent** and potentially **public** - even if it is '**protected**' in some way.

Just because something is personal in nature or an individual doesn't want people to know about it does not make it private. Social networks by their nature

blur the divide between public and private simply by being networks. Their purpose is to provide simple ways of sharing information as widely as possible and some will make information available to a far wider audience than might be expected or desired.

Seemingly innocent information, photographs, videos, opinions or comments are vulnerable to misrepresentation and unauthorised distribution via the internet.

Therefore **DO**

1. Assume everything online is permanent and effectively public
2. Make sure you consider who might see anything you post.
3. Write appropriately for your expected audience.
4. Make all staff / student online interactions meaningful and professional.
5. Consider specifically safety and reputation before posting online.
6. Take responsibility for what you post / distribute online.
7. Use the internet positively for communication, collaboration and learning.
8. Use and maintain privacy settings to protect personal information but do not rely on them.

**DON'T**

1. Post anything which might damage your own or the college's reputation
2. Redistribute any material which may harm others in any way.
3. Use the internet to form, or attempt to form, any relationship which would be otherwise inappropriate.
4. Create an online environment which invites others to post harmful content.
5. Post without thinking
6. Post without considering the safeguarding risks.

This policy will evolve over time and will be subject to regular review.

**Education**

To support this policy, an E-Safety Moodle resource has been developed to support both staff and students in their use of social media.

All students will receive education regarding the use and potential dangers of social media.

Staff are encouraged to use the resource to update their understanding and ensure they are using best practice. Staff development will be arranged to ensure staff use social media in a professional way.

Students will be advised of the how to use the internet and social media safely through both tutorials and displays and also annually as part of national 'Safer internet day'.

### 3. Code of Practice

#### 3.1 Staff Conduct

Staff are reminded that their professional responsibilities at the College require them to act professionally in their social networking and internet activities, and to create a clear distinction between their **social** and their **professional** lives. Contact with students must remain within the boundaries of their professional lives. The guiding principle here is “**think before you post**”.

Where staff make use of web-publishing and social networks for professional purposes they are expected to:

- Behave professionally and with integrity
- Adhere to college policy guidelines
- Respect their audience
- Promote productive conversations
- Protect and enhance the value of the college reputation
- Protect confidential and business sensitive information
- Be personable, add value and encourage responses
- Be proactive in correcting any errors made

Staff must not post comments or any other information on any public forum, website, social networking site or blog:

- that are unsubstantiated and/or negative about the college, their colleagues, our students, parents, or customers
- that run counter to the College’s Equality and Diversity, and Safeguarding Policies.
- that recommend or appear to endorse law breaking of any kind
- that give an account of any inappropriate behaviour

Nor should such comments be made in emails sent in an official or professional capacity.

Communications between staff and current or prospective students should only take place for **legitimate, professional reasons**. In some cases there may be a non-professional reason for a relationship to exist beyond the college (e.g. common academic interest / common membership of a club, society or team / family members). In such circumstances social communication may occur. Staff should, however, be aware of the risks involved and use their professional judgement to ensure that this communication is limited appropriately.

A member of staff inviting a current or prospective student to join a network without any professional purpose or inviting them to ‘follow’ a purely personal profile will be regarded as inappropriate (see Staff Code of Conduct). The risks in this situation are clear and there can be no justification. Where such a situation arises the college reserves the right to demand an explanation for this action and act accordingly.

Accepting any invitation to 'friend', follow or become part of a current or prospective student's personal network is also considered inappropriate.

We recognise staff may wish to take part in online communities also used by students. In such cases staff should ensure that personal information is secured. Any staff member contributing under a personal profile is obliged to ensure that minimal personal information is visible under that profile.

If a member of staff is unable to access a social media site due to it being blocked by the college network, a request to access this site should be made to the Principal who will review access to the site.

### **3.2 Official usage**

As a general principle staff should use their college contact details or a 'professional' profile for communication with current and prospective students, and ensure that any communication is both professional and necessary.

Email contact with learners, parents and other stakeholders should be channelled through the college email system. Staff should use the facility to set up a forwarding email address where access to college webmail may present a problem.

Staff should pay particular attention when replying to emails forwarded to a personal account as these will appear to the recipient as having been sent from the personal account.

The college will continue to develop the use of social media for marketing, communications and curriculum purposes.

To assist staff in posting factual and professionally presented information without using personal details the staff development co-ordinator will coordinate guidance, support and training in the management of a professional online presence and appropriate and effective use of social networks as an educational and communication tool.

**Authorised College networks** (group/page/blog) which exist for a clear professional purpose should be discussed with the Principal or Assistant Principals who will offer advice and guidance on what is acceptable.

Staff creating or participating in authorised networks should do so either anonymously, where this is possible, or under a professional profile.

**A professional profile** is where a member of staff maintains an online presence explicitly for professional purposes. This profile should minimise any information which could be used to compromise the individual and should not be used to record social activity or personal opinion but may be used to record professional information or opinion. It is important that a professional profile is not added to non-professional networks or linked to the profiles of others except

where the connection is professional. This might legitimately include links to student groups but would be unlikely to include groups of friends / family.

### **3.3 Monitoring**

Under certain circumstances the college may need to monitor staff and student email communication and use of the internet via the college's internet link. Staff and students should be aware that all use of the college internet link is governed by the JaNet Acceptable Use Policy which is available on CCO. The college also monitors internet activity using Impero software.

We recommend that staff monitor their own online presence, in particular, any material posted by others *about* them.

If staff become aware of, and / or are concerned about, any critical or unprofessional comments that are posted by colleagues they should draw these initially to the attention of the senior line manager and if necessary the Principal in order that an official response may be posted if appropriate.

It is the responsibility of line managers to monitor staff use of social networks in the workplace. In general, personal use is discouraged particularly where an alert service or other desktop 'widget' may interrupt workflow. Professional use should be transparent and any request to view interactions respected.

It is acknowledged that existing and new staff members may already have a significant online presence with membership of complex social-networks. It is the responsibility of staff to consider their existing and ongoing online activity in line with this code of practice. We anticipate that restrictions within this policy may mean that existing members of staff need to change their current practice and recognise that this will take time. For existing staff it is expected that these adjustments will be concluded within 6 months of the publication of this policy

#### **Fan Sites**

Where staff or students are the **subject** of groups, pages, sites or 'posts' over which they have no control the college commits to taking whatever reasonable steps it can to safeguard individuals and to help protect individual reputations along with the reputation of the college.

## **4. Student Conduct**

As members of the college community, students must abide by the terms of the Student Code of Conduct, respecting the rights of fellow students and staff, as well as the reputation of the college. They should think carefully about how they express themselves, and bear in mind the need to safeguard themselves. Material posted on the internet can be hard to delete and should, therefore, be considered **permanent**.

Students must not post comments on a social networking site or blog, or send text messages:

- that could be viewed as bullying or harassing another member of the college community
- that are counter to the College's Equality and Diversity policy or the Student Charter
- that explicitly encourages other members of the college community to break the law
- that are likely to bring the college into disrepute

Students should not post photos that they might not wish others to see.

Students should not invite staff to join social networks or follow purely personal profiles.

Students will be given guidance on appropriate use of the internet and e-safety through tutorial and displays and also annually as part of national 'Safer internet day'.

If a student has cause for concern regarding use of the internet or social networking, they must report the incident immediately to a member of staff. There may be occasions where this will be treated as a safeguarding issue.

**5. Associated policies: This policy must be read in conjunction with the associated policies below:**

- Safeguarding
- IT Terms and Conditions
- Data Protection Policy
- Student Disciplinary Procedures
- Staff Disciplinary Procedures
- EDI Policy
- Staff Code of Conduct

Any breach of any aspect of this social media policy by staff or students may result in action being considered under the appropriate disciplinary policy as considered necessary after appropriate investigation. Please see the college disciplinary policy for more details.

**6. Notes / Definitions**

**Open** communication takes place in a public forum which can be viewed by unknown internet users i.e. the general public

**Closed** communication is where the participants are all known to each other. Most closed communication will be between two individuals (e.g. email exchange) but would also include 'friends only' groups or sites with registered members etc.

**Public** information is that which can be accessed anonymously by internet users who are unknown to the originator.

**Private** information is that which is **only available** to a limited, **known** sub-set of internet users or **solely** by the owner of the information themselves.

The **originator** of online content is the individual who first uploads or creates the content using online tools.

**Distribution** – posting, uploading, adding, or **forwarding** digital content via electronic, web-based systems (including email) constitutes distribution of that content. A **choice** to publicly distribute private information is the responsibility of the distributor NOT the originator or the maintainer of the system used to distribute.

It is the responsibility of content originators to understand the system they are using and, where control cannot be guaranteed, to amend use of the system accordingly.

Adding content to online systems, other than those designed solely for storage purposes, will be seen as distribution of that content.

Content which is 'personal' in nature but made **available** to a public audience either deliberately or by carelessness will be considered the responsibility of the **originator/ distributor** of the content (e.g. the photographer NOT the subject of the photograph)

Whilst an initial interaction may be 'private', the content of any e-communication with a student or parent must be considered **permanent** and **de-facto public** because there can be no guarantee sought or given that the student/parent will not re-distribute content publicly.

If private information is **re-distributed** without the consent of the originator this is the responsibility of the distributor. However, where such information is inappropriate it may be necessary for the originator to defend the initial process of distribution which placed it in a vulnerable position.