

Digital Media Policy

Including Media, Internet and E-mail use



OWNED BY:		Operations Director and Head of Human Resources			
DATE OF LAST REVIEW		September 2019			
PLANNED NEXT REVIEW:		September 2022			
APPROVAL:		SLT, CIG			
APPLIES TO:	Staff	✓	Student		Public
					✓

1. Introduction

The aim of this policy is to provide guidance for employees on how they should use social media in the workplace.

The Internet, e-mail and social networking provide instantaneous channels for information sharing and communication which are freely available and accessible to all. For the College, this offers huge advantages in terms of our ability to communicate with existing, prospective and past students and their parents, our community and business organisations. 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.

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**”.

Staff are further reminded that boundaries between them and students must be maintained in the same way as expected with other interactions, students are not friends.

2. Social Media

Definition of social media

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, but not exclusively, - Twitter, Facebook and LinkedIn. Social media also covers blogs and video – and image – sharing websites such as YouTube, Instagram, SnapChat and Flickr.

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

Use of Social Media at work

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.

The College 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 College communicates with its stakeholders as well as promoting its services and facilitates communication between staff.

Employees may contribute to the College's social media activities, for example by writing for our blogs, managing a Facebook account, running an official Twitter account for the College or as part of the College (as long as it has been authorised by the Head of Marketing).

Employees must be aware at all times that, while contributing to the College'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 College in the public sphere. These safeguards include:

- professional, college branded, social media sites are set up using a relevant college email address;
- making sure that the communication has a purpose and a benefit for the College;
- obtaining permission from the Head of Marketing before embarking on a public campaign using social media;
- and getting a colleague to check the content before it is published.

Any communication that employees make in a professional capacity through social media must not:

- bring the College into disrepute, for example by:
 - criticising or arguing with anyone;
 - making defamatory comments about individuals or other organisations or groups; or
 - posting images that are inappropriate or links to inappropriate content;
- breach confidentiality, for example by:
 - revealing commercially sensitive information about the College or its staff;
 - giving away confidential information about an individual (such as a colleague, student or customer contact) or organisation (such as a rival school or college);
 - or discussing the College's internal workings or its future business plans that are not already in the public domain;
- breach copyright, for example by:
 - using someone else's images or written content without permission, with the exception of reposts or shares where such images are deemed to have been put into the public domain for this purpose;
 - failing to give acknowledgement where permission has been given to reproduce something; or
- 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 College);
- or posting images that are discriminatory or offensive (or links to such content).

Monitoring use of social media during work time

The College reserves the right to monitor employees' internet usage, but will explain to affected employee the reasons for it. The College 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;
- or acted in a way that is in breach of the rules set out in this policy.

The College reserves the right to retain information that it has gathered on employees' use of social media for a period of one year.

The College will comply with any police or safeguarding investigation by allowing such authorities access to any or all information relating to an employee's internet based activity. Access to particular social media websites may be withdrawn in any cause of misuse.

Social media in your personal life

The College recognises that many employees make use of social media in a personal capacity. While they are not acting on behalf of the College, employees must be aware that they can damage the organisation if they are recognised as being one of our employees. Bringing the College into disrepute is a disciplinary offence.

Employees are allowed to say that they work 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 College's name.

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

Any communications that employees make in a personal capacity must follow the same guidelines outlined in: Use of Social Media at Work, above.

3. E-mail

Contents of e-mail

E-mails that employees intend to send should be checked carefully. E-mail should be treated like any other form of written communication, as such, what is normally regarded as unacceptable in a letter is equally unacceptable in an e-mail communication.

The use of e-mail to send or forward messages that are defamatory, obscene or otherwise inappropriate will be treated as misconduct under the appropriate disciplinary procedure. In serious cases this could be regarded as gross misconduct and lead to summary dismissal.

Equally, if an employee receives an obscene or defamatory e-mail, whether unwittingly or otherwise and from whatever source, they should not forward it to any other address and it should be reported to the Head of Human Resources for investigation.

Statements to avoid in e-mails include those criticising the College's competitors or their staff, those stating that there are quality problems with goods or services of suppliers or customers, and those stating that anyone is incompetent

Employees are advised not to follow links in emails unless they are 100% confident of the destination, neither must they enter login details into websites unless they are 100% confident of the site. If in any doubt the IT Department must be consulted.

If the College believes there is a need to enter a staff members' email account without the express permission of the account holder, this should only be done with the authority of the Head of Human Resources; if appropriate the staff member will be advised.

CCing

Employees should exercise care not to copy e-mails automatically to all those copied in to the original message to which they are replying. Doing so may result in disclosure of confidential information to the wrong person. It also places too many e-mails in recipients' inboxes.

Sharing email addresses

Care must be taken not to divulge email address without permission, for example giving student email address to other students or parent emails with other parents, as this could be considered a data breach. To aid this it is recommended that all communication with students, parents etc. be done via the CC*Stars Journal. If that is not practical then use of 'BCC' must be used rather than adding to the 'To' of 'CC' fields.

Attachments

Employees should not attach any files that may contain a virus to e-mails, as the College could be liable to the recipient for loss suffered. The College has virus-checking in place but, if in doubt, employees should check with the IT department.

Employees should exercise extreme care when receiving e-mails with attachments from third parties, particularly unidentified third parties, as these may contain viruses.

Personal use of e-mail

Although the e-mail system is primarily for business use, the College understands that employees may on occasion need to send or receive personal e-mails using their work address. When sending personal e-mails, employees should show the same care as when sending work-related e-mails. Use of this facility must be kept to a minimum, for example a College email account should not be used for shopping sites.

Monitoring of e-mail

The College reserves the right to monitor employees' e-mails, but will explain the reasons for doing so and the Head of Human Resources will be notified in advance. The College considers the following to be valid reasons for checking an employee's e-mail if:

- the employee is absent for any reason and communications must be checked for the smooth running of the business to continue;
- the College suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or pornography (although the College understands that it is possible for employees inadvertently to receive such material and they will have the opportunity to explain if this is the case);
- the College suspects that an employee has been using the e-mail system to send and receive an excessive number of personal communications;
- the College suspects that the employee is sending or receiving e-mails that are detrimental to the College.

When monitoring e-mails, the College will, save in exceptional circumstances, confine itself to looking at the address and heading of the e-mails. Employees should mark any personal e-mails as such and encourage those who send them to do the same. The College will avoid, where possible, opening e-mails clearly marked as private or personal.

The College reserves the right to retain information that it has gathered on employees' use of e-mail for a period of one year.

4. Internet

Authorised internet use

Where an employee has been provided with a computer with internet access at their desk, they may use the internet at work.

Not everyone in the College needs access to the internet at work. Anyone who does not have access but believes that they require it should contact their manager and make a written request, setting out the reasons why access should be allowed.

Sensible internet use

Where employees are allowed access to the internet at work they are expected to use it sensibly and in such a manner that it does not interfere with the efficient running of the College. For example, where it would be quicker to make a telephone call than to engage in an internet search for the required information, then the telephone call should be made.

Employees may be called upon to justify the amount of time they have spent on the internet or the sites that they have visited.

The College encourages employees to become familiar with the internet and does not currently impose any time limitation on work-related internet use. It trusts employees not to abuse the latitude given to them, but if this trust is abused it reserves the right to alter the policy in this respect.

Removing internet access

The College reserves the right to deny internet access to any employee at work, although in such a case it will explain the reasons for doing so.

Registering on websites

Many sites that could be useful for the College require registration. Employees wishing to register as a user of a website for work purposes are encouraged to do so. However, they should ask their manager before doing this.

Licences and contracts

Some websites require the College to enter into licence or contract terms. The terms should be printed off and sent for approval in advance or e-mailed to the Operations Director before an employee agrees to them on the College's behalf. In most cases, there will be no objection to the terms and it is recognised that the free information provided by the website in question may save the College money. Employees should, however, always consider whether or not the information is from a reputable source and is likely to be accurate and kept up to date, as most such contract terms will exclude liability for accuracy of free information.

Downloading files and software

Employees should download files only on to those devices with virus checking software and should check how long with download will take. If there is any uncertainty as to whether or not the software is virus-free or whether the time the download will take is reasonable, the relevant line manager and the College's IT department should be consulted.

Using other software and hardware at work

The College does not allow employees to bring software or hardware into the office without the IT department's consent and nothing in the e-mail and internet policy modifies the College's general view on this.

Personal use of the internet

Although the e-mail system is primarily for business use, the College understands that employees may on occasion need to use the internet for personal purposes. Employees may access the internet at work for personal purposes provided that:

- such use is limited to break times only;
- the internet is not used to access offensive or illegal material, such as material containing racist terminology or nudity;
- they do not enter into any contracts or commitments in the name of or on behalf of the College;
- they do not order goods in the College name unless it is a part of the employees role to do so;
- and they do not arrange for more than small numbers, and sizes, of goods ordered on the internet to be delivered to the College address.

Monitoring of internet access at work

The College reserves the right to monitor employees' internet usage, but will explain the reasons for doing so. The College considers the following to be valid reasons for checking an employee's internet usage if the College suspects that the employee has been;

- viewing offensive or illegal material, such as material containing racist terminology or nudity (although the College understands that it is possible for employees inadvertently to view such material and they will have the opportunity to explain if this is the case);
- spending an excessive amount of time on websites that are not work related.

The College reserves the right to retain information that it has gathered on employees' use of the internet for a period of one year.

Excessive use of digital and social media at work including e-mail and use of internet

Personal use should be kept to a minimum and must not interfere with proper performance of an employee's duties. Personal use should never be made during student or visitor contact time or in public areas.

5. General

The aim of these rules is to be helpful, and to set guidelines on the use of e-mail and the internet at work for the smooth and efficient running of the business.

If there is anything in these rules that an employee considers to be unworkable or does not understand, they should notify their manager.

Self-employed contractors, agency workers or any other individuals working temporarily in the College should be made aware of the rules regarding the use of social media, e-mail and the internet.

All employees are required to adhere to this policy. Employees should note that any breaches of this policy may lead to disciplinary action. Serious breaches of this policy, for example incidents of bullying of colleagues by email or on social media activity causing serious damage to the College, may constitute gross misconduct and lead to summary dismissal.

6. Data Protection

When managing an employee's personal data information will be collected in accordance with the College's data protection policy. Data collected is held securely and accessed by, and disclosed to, individuals only for the purposes of information relating to this policy. Inappropriate access or disclosure of employee data constitutes a data breach and should be reported in accordance with the College's data protection policy immediately. It may also constitute a disciplinary offence, which will be dealt with under the College's disciplinary procedure.

7. Equality

As with all College Policies and Procedures due care has been taken to ensure that this policy is appropriate to all employees regardless of sex, age, race, marital status, maternity, ethnicity, disability, gender identity, sexual orientation or religion/faith.

The policy will be applied fairly and consistently whilst upholding the College's commitment to providing equality to all.

If any employee feels that this policy does not meet this aim please contact the College's Head of Head of Human Resources