Social and Electronic Media Policy

Formal Review Cycle:	Annual		
Latest Formal Review (month/year):	2017-10	Next Formal Review Due (month/year):	2018- 10
Policy Owner:	Director of Human Resources		
Impact Assessed by:	Yes	Impact Assessment Date:	

APPROVAL REQUIRED:

SMT Y/N	Y	SMT Date approved:	31 October 2017		
Governor Y/N	N	Committee:		Governor Date approved:	

PUBLICATION:

Website Y/N	Y	Intranet Y/N	Y	Student VLE Y/N	Y	Other:	
Area/s of Staff Intranet:	Human Resources; Marketing						

Reviewed JM Oct 2017

1. Policy Description:

1.1 This policy aims to outline the responsibilities of employees and students when accessing social media either personally or using it for College purposes. It aims to manage organisational risks when social media is used for educational, business and personal use, and to ensure that its use is acceptable to avoid bringing the College into disrepute. It supports the College policy on the use and monitoring of email and internet and the appropriate use of images.

1.2 Social media is the term used to describe the online tools, websites and interactive media that enable users to interact with each other in various ways, through sharing information, opinions, knowledge and interests. Social media involves building online communities or networks, which encourage participation, dialogue and involvement. Examples of online forums include Twitter, Facebook and LinkedIn. Social media covers blogs and video-and-image-sharing websites such as YouTube and Flickr. It is a constantly changing and expanding area.

1.3 The College recognises the value that social media can have on education, particularly for research, teaching and communication purposes if used in a responsible and professional way. While it is recognised that employees and students are entitled to a private life, the College is committed to maintaining confidentiality and professionalism at all times whilst also upholding its reputation by ensuring both employees and students exhibit acceptable behaviours.

1.4 The purpose of this Policy is to clarify the acceptable usage of e technology by both employees and students and confirm what standards of conduct are expected from employees and students in the College, to promote consistency, and to make employees and students aware of their responsibilities in maintaining a safe, professional environment and protecting themselves, and the College's reputation.

Links to other policies/documents

- Acceptable IT user policy
- Disciplinary and Dismissal Procedures
- Grievance Procedure
- Whistle blowing
- Capability Procedure
- Staff Code of Conduct
- Bullying and Harassment Policy
- Equality & Diversity Policy
- Safeguarding Policy and Safeguarding Children and Vulnerable Adults
- Health and Safety Policy

2. Context

2.1 The College is committed to high standards of health and safety and considers safeguarding of both employees and students a high priority. The College also seeks to retain its high reputation and will take appropriate action if any attempt is made to damage the reputation of the College.

2.2 The College sets out correct standards of behaviour to be adhered to when involved with social and electronic media activities. The College is also developing a Good Practice Guide to support staff in the use of electronic and social media to ensure safe standards are maintained.

2.3 Failure to observe the standards of conduct and guidelines given in this policy will be regarded as a serious misconduct and could lead to disciplinary action being taken which may include dismissal.

3. Legislation

The College will adhere to its obligations under the legislation relevant to the use and monitoring of electronic communications, which are predominantly the Regulation of Investigatory Powers Act 2000; the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000; the Communications Act 2003; Data Protection Act 1998; the Human Rights Act 1998; the Defamation Act 1996 and the Equality Act 2010.

4. Staff Social Media Policy

4.1 This policy applies to all employees employed by the College. The College is aware of its wider responsibilities to provide a positive working environment for all who work on the College premises.

4.2 Individuals are personally accountable for their behaviour and may be held liable for any breaches of this policy. All individuals who work on College premises, including agency, contract workers and volunteers are therefore expected to support the College's policy on social media.

4.3 The College Policy is that employees, and students, should have limited access to external Social media websites such as Twitter, for communication purposes, from the College's computers or IT devices, unless this forms part of the normal duties of work or for explicit educational purposes. The College has developed an internal social media platform which should be used to support communication and learning processes with students.

4.4 In order to reduce the opportunities for negative impact on student learning, the College places a block on a range of social media sites (excluding Facebook), such as Whats app, Snapchat, Instagram, Twitter, Musiacl.ly, Live.ly, Tumblr. Access is only permitted before 9.00am, at lunch time 12.00-2.00pm and after 4.30pm. Flickr (used by Media students for their course work) and You tube (regularly used for teaching materials during lessons) remain unblocked.

5.0 Acceptable Use of Social Media at Work

5.1 The College expects appropriate standards of conduct from staff reflected in the IT Acceptable Use Policy for the purpose of furtherance of the employment i.e for learning and teaching, research and administrative purposes.

5.2 The College IT Systems are therefore first and foremost business tools and for educational purposes, and as such personal usage of the systems is a privilege and not a right. However, in certain work contexts it is an important part of how the College educates, communicates and interacts with its employees/students/ customers/clients.

5.3 For Professional development in learning and teaching e.g for teaching and research purposes, teaching staff may set up a work based ID. Examples of which could be YouTube, LinkedIn and Twitter. However, permission to access external media websites will be by exception in view of the safeguarding risks and must be approved by Senior Management. Employees responsible for contributing to the College's social media activities or engaging in any electronic media on a work basis should be aware at all times that they are representing the College.

5.4 The College has developed an internal Social Media plug within the Moodle VLE system. Students and staff are able to communicate and share information within the confines of the College network. Staff and students are encouraged to use the College's internal social media platform to support communication and learning processes.

5.6 The College accepts that employees may wish to use their own personal devices, including laptops, palm-tops, hand-held devices and smartphones, to access social media websites, while at work. Employees will have limited time to use social media on their own personal equipment, in line with the College policy, restricting usage to official lunch breaks and before and after work.

5.7 Personal use of social media should not interfere with employees' work duties and responsibilities. Excessive personal use of social media websites and abuse of this policy will be considered a disciplinary offence.

6.0 Expected Standards of Conduct on Social Media Websites

6.1 Appropriate Conduct

The line between public and private, professional and personal is not easily clearly defined when using social media. If an employee identifies themselves as a member of staff at the College, this has the potential to create perceptions about the College to a range of external audiences and also among colleagues and students.

6.2 When communicating either in a professional or personal capacity, within or outside the workplace, employees must:

- Conduct themselves in accordance with other policies, procedures and the College Staff Code of Conduct, particularly when using College social media accounts to portray the College's activities, as this is an extension of the College's infrastructure
- Be professional, courteous and respectful as would be expected in any other situation
- Think carefully about how and what activities are carried out on social media websites

- Be transparent and honest. The College will not tolerate employees making false representations. If employees express personal views, it should be made clear that the views do not represent or reflect the views of the College.
- Remove or request the removal of any inappropriate comments, images or videos of them

6.3 Employees who use social and electronic media as part of their job or outside working hours whether at work or otherwise should adhere to the Staff Code of Conduct.

6.4 Employees should use the same safeguards as they would with any form of communication about the College in the public sphere. These safeguards include:

- Making sure that the communication has a purpose and a benefit for the organisation
- Obtaining permission from the Principal before embarking on a public campaign using social media
- Requesting a colleague to check the content before it is published

6.5 **Inappropriate Conduct**

6.5.1 While using social media in any capacity, employees' actions could still damage the College's reputation.

6.5.2 When communicating either in a professional or personal capacity, within or outside the workplace, employees must not conduct themselves inappropriately. If such action has a negative impact on the College's operation, this could result in disciplinary action being taken against the employee.

6.5.3 The following are examples of inappropriate conduct:

- **Engaging in activities that have the potential to bring the College into disrepute, e.g**
  - criticising or arguing with students, clients, colleagues, competitors or other organisations who have a relationship with the College;
  - publishing defamatory and/or knowingly false material about the College, other employees or students
  - posting images that are inappropriate or links to inappropriate content

- **Breach of confidentiality by disclosing privileged, sensitive and/or confidential information**, **e.g**
  - revealing trade secrets or information owned by the College
  - giving away confidential information about an individual (such as a work colleague or customer contact) or organisation (such as a rival business)
  - discussing the College's internal workings (such as business deals that it is involved in with a client) or its future business plans that have not been communicated to the public
  - commenting on any work-related matters

- **Breach of Copyright, e.g**
  - posting any material that breaches copyright legislation
  - using someone else's images or written content without permission; or
  - failing to give acknowledgement where permission has been given to reproduce something

- **Activity 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
  - posting remarks which may inadvertently cause offence and constitute unlawful discrimination, harassment and/or victimisation
  - using social media to bully or harass another individual (such as an employee or the College)
  - posting or uploading inappropriate images, photographs and/or video clips about colleagues or ex-colleagues, students or ex-students, parents or clients that are discriminatory or offensive or links to such content
  - engaging in discussions or activities which contravene the College's equality and diversity policy and may have the potential to cause serious harm to the business
  - use of offensive, derogatory or intimidating language which may damage working relationships
  - knowingly accessing, viewing or downloading material which could cause offence to other people or may be illegal

- **Blurring the boundaries of professional and personal life**
  - the development of personal relationships with students or parents should only be entered in to with extreme caution and recognition of the potential risks involved (see Staff Code of Conduct "Staff/Student relationships")
  - participating in any activity which may compromise your position at the College
  - behaviour that would not be acceptable in any other situation
  - using a College email account to create a social media account for personal use other than for educational purposes
  - using social media websites in any way which is deemed to be unlawful

The above examples are not exhaustive or exclusive.

Employees will be held personally liable for any material published on social media websites that compromise themselves, their colleagues and/or the College.

6.5.4 **Inappropriate Conduct and Excessive Use**

Any breach of this policy, including inappropriate conduct of the kind listed in section 3.8 above, or of a similar nature, and any excessive personal use of social media websites will be dealt with in accordance with the College disciplinary procedure.

Appropriate action may be taken against employees in line with the College disciplinary policy which may also result in the withdrawal of access to social media websites/withdrawal of internet access. Persistent breaches of this policy may lead to dismissal. Serious cases may be treated as gross misconduct, which may result in summary dismissal.

7. Data Protection & Monitoring

7.1 Computers are the property of the College and are primarily designed to assist in the performance of work duties. To ensure appropriate use of the internet, the College's internet software monitors all websites visited by employees for business and security purposes. Therefore, employees should have no expectation of privacy when it comes to the sites they access from College computers and devices.

7.2 The College may exercise its rights to intercept internet access under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 for the following business reasons:

- To establish the existence of facts relevant to the College's business to ascertain compliance with regulatory practices or procedures relevant to the College
- To ensure that employees using the system are achieving the standards required
- To prevent or detect crime
- To investigate or detect the unauthorised use or abuse of the telecommunications systems, including using social media websites
- To ensure effective operation of systems, e.g. to detect computer viruses and to maintain an adequate level of security

7.3 To be able to exercise its rights, the College must make all reasonable efforts to inform every person who may use the internet systems that monitoring may take place. This is stated as an express term of all employee contracts of employment.

8.0 Privacy Settings and Personal Information

8.1 Default privacy settings for some social media websites allow some information to be shared beyond an individual's contacts. In such situations, the user of the site is personally responsible for adjusting the privacy settings for the account. Information available on social media sites could be produced as evidence by either the College or employee, should it be necessary either as part of College procedures, or in legal proceedings.

8.2 Therefore, it is vital that employees are strongly encouraged to review their access and privacy settings for any social media sites to control, restrict and guard against who can access the information on those sites. Even if privacy and security settings are utilised, anything posted on social media sites may be made public by onward transmission.

8.3 Social media offers the ability to share personal information rapidly and easily. Employees should be aware of the College's Acceptable Use Policy, particularly with regard to protecting passwords and personal information to reduce the risks of abuses such as identity theft.

8.4 To avoid identity theft, employees are advised to refrain from publishing any personal or sensitive information on social media websites, e.g. date of birth, home address, telephone number or any information related to personal bank accounts.

9.0 Acceptance of "Friends"

9.1 The College accepts the positive aspects of the use of social media as part of the educational process. Social media is used by many people, particularly students to communicate with their peers and the public. To ensure professional boundaries are maintained, employees must not accept and/or invite the following individuals to become 'friends' on personal social media accounts or other online services:

- Students, including vulnerable students who are adults or children
- Ex-students under the age of 18, and
- Parents

9.2 Entering into such relationships may lead to abuse of an employee's position of trust and breach the standards of professional behaviour and conduct expected at the College. The College reserves the right to take disciplinary action if employees are found to be in breach of this policy, with the potential of dismissal for serious breaches.

9.3 Acts of a criminal nature or any safeguarding concerns may be referred to the police, Local Safeguarding Children Board (LSCB) and/or the Disclosure and Barring Service, in line with the College's Safeguarding Policy.

10.0 Use of Social Media during the Recruitment and Selection process

10.1 The College may use the internal social media website for recruitment purposes where appropriate. Any information that relates to applicants' protected characteristics under the Equality Act 2010 will not be used as part of the recruitment and selection process.

10.2 The College will only view relevant social media websites as part of the pre-employment process, i.e. those aimed specifically at the professional market and used for networking and career development (e.g. LinkedIn). Any information that relates to applicants' protected characteristics under the Equality Act 2010 will not be used as part of the recruitment and selection process.

11.0 Use of Images

11.1 North Yorkshire Safeguarding Children's Board provides advice concerning the taking and keeping of images of students. Staff who need to take pictures of students for valid reasons, e.g evidence for portfolios etc, should only do so on devices that belong to the College. Staff should never use their own mobile phones or devices to take images of students. In order to enable staff to still collect photographic evidence, they should use College owned cameras only.

11.2 Images are used in a range of contexts across the College, both by students and staff. These uses can be categorised into four groups: images used by the organisation, images used by marketing, images used to support teaching and learning and images used by students to support the achievement of learning outcomes

11.3 Images used by the organisation include ID Cards. The College records an image of every student and staff member for the purpose of identification and to support the safeguarding of all within the College community. These images are kept within secure storage and form part of the student record. The protection of such images

and data fall within the responsibility of the Management Information Services Manager and under the Data Protection Act.

11.4 Student images generated for ID purposes are held securely on E-pro. Access to these images is limited to staff with Enhanced DBS clearance. These images should not be used for any other purpose than ID.

11.5 Images collected through Closed Circuit Television (CCTV)

11.5.1 CCTV footage is recorded in several areas of the College. Only specified members of staff are allowed to view CCTV footage, all of whom have Enhanced DBS clearance. If it is necessary for any other member of staff to view the footage, it will be the responsibility of one of the specified members of staff to ensure that this has been approved by the Chair of the Safeguarding Committee and that they have sufficient DBS clearance.

11.5.2 In addition to the above, members of the Police will also have access as part of any investigation they may be carrying out; at such times these personnel will sign onto site as visitors and be accompanied by an authorised member of College staff.

11.5.3 Copies of relevant CCTV footage may be copied and released to the Police in order to provide evidence for an investigation. A log of all receipts for footage provided is kept by the Technology Systems Development Manager.

11.5.4 CCTV images will be retained for four weeks.

11.6 Images used within Marketing.

11.6.1 On induction students are asked to consent to their image (still and moving) being used to market and promote the College through the social media, on the website and within the College premises. Students over the age of 16 must give opt in consent for their images to be used. Consent forms are registered on the College system and held by the Marketing Department. Any students not giving consent are then held on a database, this database is only accessible by the Child Protection Officer. Reasons for consent not being given may include those on an at risk register, have a student disciplinary record, refuse to give consent or for unspecified reasons.

11.7 Images used to support teaching and learning.

11.7.1 During induction students will be reminded of the image consent and advised as to where it will be used within the curriculum. The member of teaching staff responsible for the module or unit will need to advise the students what the purpose is, where the image will be stored and where it will go. Should the image be inappropriate for viewing or for assessment purpose then it will not be permitted to be used.11.7.2Within curriculum planning, teaching staff must clearly identify within the planning documentation what media will be used and the purpose for the use, this may be for teaching, assessment or verification purposes. The member of staff must provide assurance that any images or student work will be viewed and stored safely.

11.7.3 Wherever possible staff should use Moodle based activities in conjunction with the course VLE and Student e-ILP. If College systems do not meet the curriculum and/or

Awarding Organisation needs, staff must carry out a risk assessment on any new technology and/or online platforms and consult the Technology Systems Development Manager for advice and guidance. Social media websites within the public domain should not be used.

11.7.4 Staff will provide information to students regarding e-safety and the safe storage of stills and moving images. Staff will also maintain the integrity of the College and students by ensuring that when images are taken the dress code is appropriate, the correct equipment and personal protective equipment (PPE) are worn, Health and Safety procedures are adhered to and the images in the background are appropriate and representative.

11.7.5 If members of staff fail to comply with these guidelines and appropriate conduct referred to in 3.7 the staff disciplinary procedure will be implemented.

11.7.6 All students and staff must accept full liability for any material they choose to post on an internal Social Media Site. This includes recognising that they alone will be accountable for any legal action or threat of legal action arising from their words or pictures or other material.

11.7.7 If inappropriate material is identified or reported as having been posted the College will make reasonable attempts to remove it or have it removed as soon as possible after it becomes aware of the material.

11.7.8 The College will take reasonable steps to try to prevent incorrect or illegal content. A statement is included on each site confirming that the responsibility for content rests with the individual. If any incorrect or illegal content is reported to the College reasonable steps will be taken to remove it within a reasonable timescale.

11.7.9 Staff who are authorised to set up such a site must carry out reasonable periodic checks for any material that may be inappropriate – and must respond immediately if such material is reported to them whether formally or informally, in writing, by email, orally or in any other medium.

11.7.10 Staff who become aware of any unacceptable material should contact their Line Manager immediately in the first instance.

11.8 Images taken by students

11.8.1 Images taken by students to support learning and assessment

Students may be requested by their tutors, as part of their studies to record still or moving images or sound, using either their own or College equipment. In all circumstance students must be given advice as to how it will be used and stored. Failure to comply with instructions may result in student disciplinary action

11.8.2 Images taken by students in a social context i.e not directed by a tutor

The College will not tolerate any defamatory or inappropriate use of images and sound and any such instance will result in disciplinary actions. Students can access guidance on Social Media etiquette and their legal responsibilities via induction, tutorial programmes and the College VLE.

12.0 Student Social Media Policy

12.1 Whilst the College recognises the value of new technologies, including social media, if used in a responsible and professional way, the College is committed to safeguarding and maintaining confidentiality and professionalism at all times whilst also upholding its reputation by ensuring both employees and students exhibit acceptable behaviours.

12.2 The College is committed to taking all reasonable steps as far as it is reasonably practicable to eliminate all risks of harm to students.

12.3 The College Policy is that students should have limited access to external Social media websites such as Twitter, for communication purposes, from the College's computers or IT devices, unless this forms part of the normal duties of work or for explicit educational purposes. The College has developed an internal social media platform which should be used to support communication and learning processes with students.

12.4 In order to reduce the opportunities for negative impact on student learning, the College places a block on a range of social media sites (excluding Facebook), such as What's app, Snapchat, Instagram, Twitter, Musiacl.ly, Live.ly, Tumblr. Access is only permitted before 9.00am, at lunch time 12.00-2.00pm and after 4.30pm. Flickr (used by Media students for their course work) and You tube (regularly used for teaching materials during lessons) remain unblocked.

12.5 Students are responsible for using the College IT systems and mobile devices for educational purposes in accordance with the College's IT Acceptable Use Policy, which they must agree to and sign before access to the College network is permitted.

12.6 A link to the College e-Safety rules will appear when users log on to the College's VLE which are also highlighted in posters and leaflets around IT areas and work stations. Within classes, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded.

12.7 The College encourages training and education for students to increase their awareness for their own protection and safety. This will provide them with the skills to be able to identify risks independently and manage them effectively.

12.8 Students are responsible for accessing e-safety awareness raising as part of their tutorial programme and particularly at the start of the year. They are expected to seek help and follow College procedures where they have concerns about e-safety, where they believe an e-safety incident has taken place involving them or another member of the College community.

12.9 Issues associated with e-safety apply across the curriculum and students should receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies. Students are strongly advised to review their privacy settings for their own protection.

12.10 There are clear lines of responsibility for e-safety within the college. The first point of contact for students would normally be the Course Tutor or Progress Coach who should inform the Child Protection Officer in the Student Services Department. All staff are responsible for ensuring the safety of students and should report any

concerns immediately to the Child Protection Officer. All teaching staff should be made aware of the need to draw attention to the students' e-responsibility (where the opportunity arises) and to adhere to the Child Protection reporting procedure.

12.11 Where any report of an e-safety incident is made, all parties should know how this will be followed up. Appropriate support or guidance may be sought from external agencies if necessary.

12.12 Expected standards of conduct from students

12.12.1Students must adhere to College policies at all times when using the internet and/or mobile technologies.12.12.2 The College expects appropriate standards of conduct from students reflected in the IT Acceptable Use Policy for the purpose of furtherance of the course of study i.e for learning and research purposes.

12.12.2Whilst engaged in using social media for personal use the College expects students to be respectful and courteous towards others. The following are examples of inappropriate conduct:

- Publishing defamatory and/or knowingly false material about the College, College employees or other students
- Posting images that are inappropriate or links to inappropriate content
- Disclosing privileged, sensitive and/or confidential information
- Posting any material that breaches copyright legislation
- Using someone else's images or written content without permission
- Failing to give acknowledgement where permission has been given to reproduce something/citing references inappropriately
- Making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age
- Posting remarks which may inadvertently cause offence and constitute unlawful discrimination, harassment and/or victimisation
- Using social media to bully or harass another individual (such as another student or College employee)
- Posting or uploading inappropriate images, photographs and/or video clips about students or College employees that are discriminatory or offensive or links to such content
- Engaging in discussions or anything which contravene the College's Single Equality Scheme and may have the potential to cause serious harm to the business
- Knowingly accessing, viewing or downloading material which could cause offence to other people or may be illegal
- Using a College email account to create a personal social media account
- Using social media websites in any way which is deemed to be unlawful

The above examples are not exhaustive or exclusive.

12.12.3Disciplinary action may be taken against students in line with the College's Student Disciplinary Policy. Serious cases may be treated as a Level 3 Disciplinary, which may result in expulsion from the College. Serious breaches of conduct could involve the police.

13.0 Cyberbullying

13.1 Cyberbullying is the use of Information and Communications Technology, particularly mobile phones and the internet, deliberately to upset someone else. Cyberbullying can take different forms such as threats and intimidation; harassment or 'cyberstalking', defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images; and manipulation. The person being bullied will usually have examples of texts, emails and should be encouraged to keep these to aid any investigation. A person experiencing cyberbullying should not reply or retaliate, should use 'blocking' or removing from 'friends' contact and take steps to identify the person responsible. Such behaviour should be reported to the Course Tutor initially or directly to the Child Protection Officer.

14.0 Responsibilities

14.1 All employees and students are responsible for complying with the requirements of this policy and for reporting any breaches of the policy to their Line Manager/Course tutor.

14.2 Employees must be vigilant to the risks of radicalisation and extremism via social and electronic media and carry out preventative action to safeguard students from terrorism.

14.3 If employees or students have concerns about information or conduct on social media sites that are inappropriate, offensive, demeaning or could be seen to be bullying, this should be reported to their Line Manager /Course tutor and in turn the Child Protection Officer immediately.

14.4 The Technology Services Department is responsible for maintaining the College's computer systems and for supporting employees in the proper usage of the systems. System checks and appropriate monitoring is carried out using filtering as a means of restricting access to harmful content to ensure learners are safe from terrorist and extremist material when accessing the internet, hence preventing them from being drawn into terrorism.

14.5 The Child Protection Officer has the responsibility for investigating e safety breaches of conduct.

14.6 The Safeguarding Committee is responsible for drafting, updating, monitoring and reviewing this policy.