EASTLEIGH COLLEGE

COMMUNICATION POLICY FOR STAFF

1. Introduction

These guidelines detail the methods of communications available to staff and the expected standards when communicating with other staff, students, external partners and employers. This includes communication by post, e-mail, text messaging, telecommunications, social media, general use of IT and the college network and Moodle.

The Guidelines apply to all members of staff inclusive of Board appointments as defined in the College's Instruments & Articles of Government.

Although these Guidelines refer to employees throughout, the College is aware of its wider responsibilities to provide a positive working environment for all who work within the remit of the College. Employees must adhere to the principles of e-safety by behaving appropriately and within the law.

Individuals are personally accountable for their behaviour and may be held liable for any breaches of these Guidelines. All individuals who work in the name of Eastleigh College either on College premises or at other locations, including agency, contract workers and volunteers, are therefore expected to support the College's Guidelines on the use of College IT, network, internet, social media, email and telecommunications.

In order to safeguard the College and its employers, staff must adhere to all relevant legislation and the principles of e-safety as described in the Data Protection Guidelines. In addition this guidance should be read in conjunction with College policies: Dignity at Work, Staff Code of Conduct, Personal Relationships Guidelines and the Disciplinary Procedure. By using the College IT facilities staff are agreeing to adhere to this document and associated policies and legislation.

2. Appropriate use

The College provides access primarily for business and educational purposes, however appropriate personal use is permitted to a minimum and is considered reasonable without impacting on College duties. If you are unsure whether an activity constitutes appropriate or inappropriate use check with your line manager or the IT helpdesk helpdesk@eastleigh.ac.uk. Any concerns regarding safeguarding/child protection should be referred to the Safeguarding Team by calling the safeguarding phone on 07535 056856.

All communication with students in any medium must adhere to the Eight Principles of Data Protection. In particular, staff must not disclose the personal details of any other student or staff member to another without the first individual's explicit consent. Please note that the College may contact the named next of kin for students who are under 18 when their course starts, and may contact employers who are sponsoring students through payment of fees or time release. For further details see the Data Protection Policy and Guidelines on the L:Drive at Policies and Procedures.

All communication with students must be objective and professional and in keeping with maintaining the reputation of the College. All communication with students must use proper grammar and spelling, and be laid out in a manner appropriate to the format of the medium being used.

3. IT, network, internet, social media, email and telecommunications guidelines for staff

The College provides access to its IT, network, internet, social media, email and telecommunications primarily for business and educational purposes. If you are unsure whether an activity constitutes appropriate College use, consult your line manager.

3.1 Aims and objectives

These Guidelines aim to outline the responsibilities of employees when accessing College IT, the network, internet, social media, email and telecommunications either personally or using it for College purposes. It aims to manage organisational risks when College IT, the network, internet, social media, email and telecommunications is used for both business and personal use, and to ensure that its use is acceptable to avoid bringing the College into disrepute.

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 social media sites are:

- Facebook
- YouTube
- Twitter
- LinkedIn
- Online messenger service (ie BBM)
- Blogs
- Skype
- Facetime
- Google +

The above examples are not exhaustive or exclusive.

The College recognises the value that social media can have to our business and our students if used in a responsible and professional way. While it is recognised that employees 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 employees exhibit acceptable behaviours.

3.2 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 Computer Misuse Act 1990; the Communications Act 2003; Data Protection Act 1998; the Human Rights Act 1998; the Defamation Act 1996, the Equality Act 2010 and the Counter-Terrorism and Security Act 2015.

3.3 Data protection and monitoring

The College IT facilities and network is primarily designed to assist in the performance of work duties. To ensure appropriate use of the internet, the College monitors all websites visited by employees, for business, security and safeguarding purposes, including the Wi-Fi ‘guest’ network. Therefore, employees should have no expectation of privacy when it comes to the sites they access from College computers and the network. Please see the College’s Data Protection Policy and Guidelines.

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, eg to detect computer viruses and to maintain an adequate level of service and security

3.4 Confidential information

Unless authorised to do so, employees are prohibited from using College IT, the network, internet, social media, email and telecommunications to transmit confidential information to outside parties. Employees may not access, send, receive, solicit, print, copy or reply to confidential or proprietary information about the College, employees or other business associates unless authorised to do so.

Confidential information shall include (but shall not be limited to) the following:

- The College's marketing strategies and business plans
- Any information relating to a proposed reorganisation, expansion or contraction of the College's activities including any such proposal which also involves the activities of any other corporation or organisation
- Financial information relating to the College (save to the extent that such information is included in published audited accounts)
- Details of employees of the College, the remuneration and other benefits paid to them and their experience, skills and aptitudes
- Personal details of students
- Any information which you have been told is confidential or which you might reasonably expect to be confidential
- Any information which has been given to the College in confidence by students or other persons, companies or organisations
- Any information that is commercially sensitive

For guidelines on Data Protection and Freedom of Information see the Policies and Procedures section of the L:Drive.

3.5 Privacy settings and personal information

Access to College IT, the network, internet, social media, email and telecommunications is provided as a tool primarily for the College's business. Under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the College has the right to monitor any and all aspects of its telephone and computer systems that are made available to you and to monitor, intercept and/or record any communications made by employees, including telephones, email or internet communications.

In addition, the College wishes to make you aware that Closed Circuit Television (CCTV) is in operation for the safeguarding of employees and students.

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 employees should it be necessary, either as part of College procedures, or in legal proceedings.

Therefore, it is vital that employees and students are strongly encouraged to regularly 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.

Social media offers the ability to share personal information rapidly and easily. Employees should protect themselves with regard to protecting passwords and not publish personal information to reduce the risks of abuses such as identity theft.

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

For more information please visit 'Using Facebook to Support Teaching & Learning' within the Moodle Staffroom, or contact the E-Learning Facilitator, who will be able to advise further on protecting staff identity on social media sites.

3.6 Pageone text messaging

Student details and mobile phone numbers are updated by the IAG team at point of application, interview and enrolment. At other points, details can be updated by the member of staff completing a change of information form which should be passed to contracts and learning data. Communication with students via text messaging will normally be the responsibility of the Learner Mentor team and/or IAG & Admissions. A weekly import of student mobile phone numbers from the MIS system 'ProSolution' into the 'PageOne' text messaging system will be carried out by Computer Services.

Staff details and phone numbers are recorded by HR in 'HR Select' and updates carried out by Human Resources. Communication with staff will normally be the responsibility of the HR team. Computer services will systematically import staff mobile numbers from HR Select into PageOne text messaging system.

Computer Services are responsible for the system maintenance and administration, including billing. Computer Services Manager will process urgent authorised texts out of normal College hours.

3.7 Acceptable use of social media at work

The College IT Systems are first and foremost business tools, and as such personal usage of the systems is a privilege and not a right. Employees are permitted to make reasonable and appropriate use of social media websites where this is part of the normal duties of their work. It is an important part of how the College communicates and interacts with its employees/students/customers/clients.

Employees responsible for contributing to the College's social media activities should be aware at all times that they are representing the College. Employees, who use social media as part of their job, should gain guidance from the Safe Use Guidelines on Moodle, alternatively contact the E-Learning Facilitator.

The College accepts that employees may wish to use social media channels as a way of communicating personally with the public and/or friends; however its use at work should be restricted to the terms of these Guidelines. Employees are permitted to make reasonable and appropriate use of social media websites for personal use from the College's IT network. Personal use of social media should be limited to when employees are between appointments when travelling and/or times when they are not on duty (before and after work and lunch breaks).

Employees may wish to use their own personal devices, including laptops, palm-tops, hand-held devices and smart phones to access social media websites while at work. Employees should limit their use of social media on their own personal equipment to their lunch breaks and/or when between appointments when travelling and/or times when they are not on duty (before and after work).

Personal use of social media should not interfere with employees' work duties and responsibilities. Excessive personal use of social media website and abuse of these Guidelines will be considered a disciplinary offence.

3.8 Expected standards of conduct on social media websites

By accessing the College's IT network, Wi-Fi, or internet system, you agree to adhere to this document. You also agree to report any network or internet misuse to your line manager. Misuse also includes any breach of the document that may harm the reputation of the College, another person or another individual's property.

3.8.1 Appropriate conduct

The College is aware that there may be occasions when employees may need to access the network, internet, social media, email and telecommunications for personal communication. Personal use of the network, internet, social media, email and telecommunications should be kept to a minimum and is considered reasonable providing this does not impact on College duties and does not contravene these Guidelines.

The line between public and private, professional and personal is not always 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.

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 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.

3.8.2 Inappropriate conduct

While using College IT, the network, internet, social media, email and telecommunications in any capacity, employees' actions can still damage the College's reputation.

When communicating either in a professional or personal capacity, within or outside the workplace, employees must conduct themselves in a professional manner, (guidance can be sought from the Staff Code of Conduct). The following are examples of inappropriate conduct:

- Engaging in activities that have the potential to bring the College into disrepute.
- Breach of confidentiality by disclosing privileged, sensitive and/or confidential information.
- Making comments that could be considered to be bullying, harassing or discriminatory against any individual, eg cyber bullying in any form.
- Posting remarks on social media which may inadvertently cause offence and constitute unlawful discrimination, harassment and/or victimisation.
- Accessing or uploading inappropriate comments, controversial or offensive materials including images, photographs and/or video clips about colleagues or ex-colleagues, students or ex-students, parents or clients.
- Knowingly accessing, viewing or downloading material which could cause offence to other people or may be illegal.
- Downloading or posting any material that breaches copyright legislation.
- Uploading a virus, harmful component or corrupted data.
- Publishing defamatory and/or knowingly false material about the College, other employees or students.
- Engaging in discussions or anything which may contravene the College's equality and diversity guidelines and may have the potential to cause serious harm to the business.
- Use of offensive, derogatory or intimidating language which may damage working relationships.
- Blurring the boundaries of professional and personal life.
- Engaging in private commercial activity or soliciting money for personal gain.
- Pursuing personal relationships with students, ex-students or parents through social media (see Personal Relationships Guidelines).
- Participating in any activity which may compromise your position at the College.
- Behaviour that would not be acceptable in any other situation.

- Inappropriate commenting on any work-related matters.
- Doing anything that may conflict with the interests of the College.
- 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.

3.8.3 Acceptance of 'friends'

The College encourages the positive use of social media as part of the educational process in accordance with the Safe Use Guidelines on Moodle. Social media is used by many people, particularly students to communicate with their peers and the public.

Students may wish to form personal relationships with College employees, however to ensure professional boundaries are maintained, College employees must not accept and/or invite the following individuals to be 'friends', 'followers' or similar 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

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 these Guidelines, with the potential of dismissal for serious breaches.

Acts of a criminal nature or any safeguarding concerns may be referred to the Police, Local Safeguarding Children Board (LSCB) and/or the Independent Safeguarding Authority (ISA).

Employees may also wish to form personal relationships with colleagues; in these cases employees are encouraged to consider professional boundaries and information posted by themselves and other 'friends' which may come under the inappropriate conduct above. Individuals are encouraged to think about options such as using the different levels of privacy settings on social networking sites, which will give access to a limited profile, and will also restrict third parties from gaining access to private information, via mutual social networking site contacts. Further guidance on personal relationships can be sought from the College's Personal Relationships Guidelines or by contacting the HR Manager. Employees may also wish to speak to the College's E-Learning Facilitator for more information regarding protecting their online profile.

3.9 Use of social media during recruitment and selection process

At no stage during the recruitment process will the HR Department or line managers conduct searches on prospective members of staff on social networking websites; however the College may use appropriate social media to advertise posts. This is in line with the College's equality and diversity guidelines. 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.

3.10 Use of mobile technology and communication equipment whilst driving

The use of mobile technology whist driving is illegal. In addition, research suggests that even the use of hands-free technology is distracting and so this is also not permitted in College vehicles or whilst on College business.

4. Inappropriate conduct and excessive use

Any breach of these Guidelines, including inappropriate conduct of the kind listed in section 7 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.

All employees should be aware that failure to comply with this document may result in the withdrawal of services and/or result in disciplinary action up to and including dismissal. In serious cases the Police will also be involved.

NB The College may suspend access at any time for technical reasons, breach of guidelines or other concerns.

5. Responsibilities

The Human Resources Department in liaison with Computer Services are responsible for updating, monitoring and reviewing these Guidelines.

All employees are responsible for complying with the requirements of these Guidelines and for reporting any breaches of the Guidelines to their line manager.

If employees have concerns about information or conduct on accessing the network, internet, social media, email and telecommunications that are inappropriate, offensive, demeaning or could be seen to be bullying, these concerns should be reported to their line manager or the Human Resources Manager immediately. Safeguarding and/or Child Protection matters should be referred to the Safeguarding Team by calling the safeguarding phone on 07535 056856.

6. Further reference

- Dignity at Work Procedure
- Staff Code of Conduct
- Personal Relationships Guidelines & Guidance
- Disciplinary Procedure & Guidance Notes
- Safeguarding and Child Protection Procedure

Approved by SMT, 5 October 2016