E-mail and internet policy

Most employees have access to e-mail and the Internet for exclusive use in connection with the College's business and as part of the normal execution of their job duties. The purpose of these rules is to protect the College's legal interests. Unregulated access increases the risk of employees inadvertently forming contracts through e-mail and increases the opportunity for wrongful disclosure of confidential information and trade secrets. In addition, carelessly worded e-mail can expose the College to an action for libel. As such, e-mail to clients and employees must follow the College's designated house style, which will be supplied to authorised users. Failure to follow house style is a disciplinary matter and will be dealt with under the College's disciplinary procedure. E-mail should not be used for unsolicited correspondence or marketing campaigns and employees may not commit the College financially by e-mail unless they have been granted a specific level of delegated authority to do so.

Employees who are authorised users are not permitted to surf the Internet or to spend excessive time "chatting" by e-mail for personal and private purposes during their normal working hours. Employees are also prohibited from using e-mail to circulate any non-business material. Not only does excessive time spent online lead to loss of productivity and constitute an unauthorised use of the College's time, sexist, racist or other offensive remarks, pictures or jokes sent by e-mail are capable of amounting to unlawful harassment. As "cyber bullying" is an emerging risk, employees are also prohibited from using the College's electronic communications as a means of intimidating or bullying employees or third parties. Employees who are discovered contravening these rules may face serious disciplinary action under the College's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

Use of instant messaging systems must be expressly approved in advance by the employee's line-manager.

Employees who are authorised users are permitted to surf the Internet for personal purposes outside their normal working hours. The College considers acceptable personal use of the Internet to include activities such as personal online shopping, booking holidays and banking. It does not include visiting online gambling sites or participating in online gaming. Employees should note that any purchases or other transactions made online whilst at work are made entirely at their own risk. Employees must not use their work e-mail address to make orders for personal goods and services.

Employees who are authorised users are also only permitted to log on to Ebay, social networking and video sharing websites such as Facebook, MySpace, Bebo, Twitter and YouTube or use the College's IT systems to keep a personal weblog ("blog") outside their normal working hours. The College nevertheless reserves the right to restrict access to websites of this type at any time.

Logging on to sexually explicit websites or the downloading and/or circulation of pornography or other grossly offensive, illegal or obscene material or using the Internet for gambling or illegal activities constitutes gross misconduct and could render the employee liable to summary dismissal under the College's disciplinary procedure. "Rogue" websites exist that appear harmless but instead direct the user automatically to another website that may contain inappropriate material. If this occurs, please contact the IT department immediately. The majority of "rogue" e-mails are filtered before they reach individual PCs and then the junk facility filters them out. The IT department constantly monitors the situation.

Social networking and video sharing websites

The use of social networking and video sharing websites and blogs is permitted for genuine college related reasons. Care must be taken and advice sought from the IT department over security issues where these are evident.

When logging on to and using social networking and video sharing websites and blogs, including personal use on non-College computers outside the workplace, employees must not:

- write about their work for the College in a negative manner - and they must ensure also that any views expressed are clearly stated to be theirs alone
- conduct themselves in a way that is detrimental to the College or brings the College into disrepute

- allow their interaction on these websites or blogs to damage working relationships between employees, students, patients and clients of the College
- include personal information or data about the College's employees, contractors, suppliers, employees or clients without their express consent (an employee may still be liable even if employees, students, patients, contractors, suppliers, employees or clients are not expressly named in the websites or blogs as long as the College reasonably believes they are identifiable) - this could constitute a breach of the Data Protection Act 1998 which is a criminal offence
- make any derogatory, offensive, discriminatory or defamatory comments about the College, its employees, students, patients, contractors, suppliers, employees or clients (an employee may still be liable even if the College, students, patients, its employees, contractors, suppliers, employees or clients are not expressly named in the websites or blogs as long as the College reasonably believes they are identifiable)
- make any comments about the College's employees that could constitute unlawful discrimination, harassment or bullying contrary to the Equality Act 2010 - you can be personally liable for your actions under the legislation
- disclose any trade secrets or confidential or sensitive information belonging to the College, its employees, contractors, suppliers, employees or clients or any information which could be used by one or more of the College's competitors, for example information about the College's work, its products and services, technical developments and staff morale
- breach copyright or any other proprietary interest belonging to the College.

Employees should remember that social networking websites are a public forum, even if they have set their account settings at a restricted access or "friends only" level, and therefore they should not assume that their entries on any website will remain private.

Employees must also be security conscious when using social networking websites and should take appropriate steps to protect themselves from identity theft, for example by restricting the amount of personal information they give out, such as date and place of birth, schools attended, family names and favourite football team. This information may form the basis of security questions and/or passwords on other websites, such as online banking.

If employees are asked to contribute to an official blog or newsfeed connected to the College, then special rules apply and the employee will be briefed in detail about what to write.

Employees who are discovered contravening these rules, whether inside or outside the workplace, may face serious disciplinary action under the College's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

Downloading information from the Internet and file sharing

Due to our faster computer networks, employees may be tempted to make illegal downloads of material that is subject to copyright. This includes, but is not limited to, music, film and business software. As this and any subsequent file sharing of this material constitutes an infringement of copyright, it is prohibited on any College computer. This also applies to any download or dissemination of material made outside of normal working hours. Any breach is likely to lead to disciplinary action being taken.

You may need to download documents and information from the Internet in order to undertake your job duties. You should only download documents and information that you are sure about and which is required to fulfil the job duties you are undertaking. With the rapid spread of computer viruses via the Internet, care should be taken when accessing websites that you are not familiar with or when downloading documents or information.

You must not download any programs from the Internet without the prior approval of the IT department. Some websites require additional add-in software to display the page completely. These add-ins usually provide additional sound or visual effects. Under no circumstances should these be downloaded without the prior approval of the IT department.

Downloading from sites for legitimate research, teaching & learning and administrative purposes which require College administrative rights must be referred to the IT department.

E-mail and Internet monitoring

The College reserves the right to monitor employees' internal and external e-mails and use of the Internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes for such monitoring are to:

- promote productivity and efficiency
- ensure the security of the system and its effective operation
- ensure there is no unauthorised use of the College's time, e.g. that an employee has not been using e-mail to send or receive an excessive number of personal communications
- ensure the smooth running of the business if the employee is absent for any reason and communications need to be checked
- ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to unlawful harassment
- ensure that inappropriate websites are not being accessed by employees
- ensure there is no breach of commercial confidentiality.

Communications of a sensitive or confidential nature should not be sent by e-mail because it is not guaranteed to be private.

When monitoring e-mails, (this is undertaken on the authority of the principal or the Executive Director of Administration) the College will, except in exceptional circumstances, confine itself to looking at the address and heading of the e-mails. However, where circumstances warrant it, the College may open e-mails and access the content. In this case, the College will avoid, if possible, opening e-mails clearly marked as private or personal.

The College reserves the right to restrict, deny or remove e-mail or Internet access to or from any employee.

Reading and storing e-mails

You must check your mailbox regularly during normal working hours. It is your responsibility to read and action any e-mail you receive.

The e-mail system is not to be used as a storage area. Unwanted messages should be deleted completely. Important information or files should be saved into your private or communal data areas or into e-mail folders.

If you are going to be out of the office for a day or longer and as such you will be unable to check your e-mail, you should switch on your "out of office assistant" message. E-mail received in your absence will not normally be read by other members of staff unless you have specifically requested a colleague to undertake this task. However, e-mail may need to be checked by managers for business-related reasons when the employee is absent for any reason. It may therefore be unavoidable that some personal e-mails might be read in these circumstances.

E-mail viruses and spam

All incoming and outgoing external e-mails are checked for computer viruses and, if a virus is found, the message will be blocked. E-mails may also be checked for other criteria, for example, having an attached image file or containing offensive or inappropriate material or including a "banned" word or from a "banned" user under the criteria in the College's spam software which indicates the message is spam. Again, the e-mail will be blocked. The College reserves the right for the IT department to block and then read these messages to ascertain whether they are business-related.

If you receive an e-mail or data file that is in a format or comes from a source that you do not recognise, do not open the item but contact the IT department immediately. Any executable (.exe) files received by e-mail must be referred to the IT department for clearance before any other action is taken.

If you receive any unsolicited e-mails or spam that manages to bypass the College's spam software, you must not respond in any way. Please forward the e-mail to the IT department and they will add the sender to the list of banned users. Some spam e-mails may offer the option to opt out of receiving them. Be

aware that this is sometimes used as a way by unscrupulous spammers of validating a live e-mail address.

Temporary workers

From time to time, the College may need to use temporary staff in order to cover busy periods or annual leave. Should any temporary worker need to use a computer with access to e-mail and the Internet as part of their job role, the manager responsible for their day-to-day supervision will be required to bring this policy and its contents to their attention.

Contravention of this policy

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under the College's disciplinary procedure.

Jerry Lewis
Executive Director of Administration
14th November 2011.
Reviewed 2006