Staff IT Network Acceptable Use Policy

Authored by: James Drain
Publish: 23/12/2015 14:47:00
Last update: 23/12/2015 14:54:42

All staff will be required to accept this policy if they wish to use the College telecommunications (telephone) and computer system and machines or are required to do so in order to perform their appointed role.

IT Network Acceptable Use Policy

Acceptable Telecommunications, Network and Internet Use Policy - For Staff

1. **The Staff AUP**

All staff will be required to accept this policy if they wish to use the College telecommunications (telephone) and computer system and machines or are required to do so in order to perform their appointed role.

Any student or member of staff wishing to have further guidance on the statement and the policy before they agree should contact the Computing Services Department on x4832

The Computer Misuse Act regulates access to computers and unauthorised access to third-party computers may constitute a criminal offence and is broken into 3 sections:-

1. unauthorised access to computer material, punishable by 6 months imprisonment or a fine "not exceeding level 5 on the standard scale"; (currently £5000);
2. unauthorised access with intent to commit or facilitate commission of further offences, punishable by 6 months/maximum fine on summary conviction or 5 years/fine on indictment;
3. unauthorised modification of computer material, subject to the same sentences as section 2 offences

The telecommunications and computer system is owned by the College and is made available to staff primarily to enhance their professional activities including teaching, research, administration and management and to students to further their education.

Breaches of the Policy and conditions of use will result in appropriate disciplinary action being taken.

2. **Accounts**

Access should only be made via the authorised account and password, which should not be made available to any other person.

Any person who knowingly logs on to any College system under an unauthorised or 'borrowed' ID, or who tries to gain access to any areas of the system that they are not usually entitled to, is liable to prosecution under The Computer Misuse Act (1990). This could incur a 5,000 GBP fine or 6 months imprisonment. This would apply to any students trying to gain access to staff computers, unauthorised users trying to connect to financial or personnel databases (inside or outside the College) or staff using someone else’s account.

Activity that threatens the integrity of the College ICT systems, or that attacks or corrupts other systems, is strictly forbidden.

Users should save work to a network drive and not the local computer drive (the C: drive). Backups of network drives are taken for disaster recovery purposes.

3. **Examination of files**

The College reserves the right to examine or delete any files and e-mails that may be held on its computer system or to monitor any network use and Internet access within guidelines of the Regulation of Investigatory Powers (RIP) Act 2000, Data Protection Act 1998 and the Freedom of Information Act 2000.

4. **Telephone communications**

Telephone calls are not intercepted or recorded by the College, but telephone usage may be monitored on the basis of cost, duration or frequency.

5. **Copyright**

Copyright of materials and intellectual property rights must be

respected. No copyright DVDs, CDs, software or other material may be copied using computer equipment. Any copyright files identified on the College network may be deleted without warning.

6. **Emails and texts**

The College email system should be used for business purposes only.

Users are responsible for the content of all emails and text messages sent. Professional levels of language and content should be applied in all cases. Users should be aware that if emails are forwarded to a third party they remain responsible for any content they have emailed.

Sending anonymous emails or texts, forwarding chain letters or spam content is strictly forbidden. It is also forbidden to send an email or communication impersonating another individual.

7. **Social media (Facebook, snapchat, dating websites, Twitter etc), websites and blogs**

Users must not submit or post material that is harassing, libellous, abusive, threatening, harmful, vulgar, obscene, sexually explicit or otherwise objectionable in any manner or nature to social media, blogs and web sites, including those which form part of the College Intranet or websites.

Users must not impersonate other individuals when submitting to social media, blogs and web sites.

Users must not submit or post advertisements or commercial solicitations to College forums, blogs and web sites;

8. **Cookies on the intranet**

The intranet and associated internal online services require the use of cookies in order to operate correctly. We only use cookies that are essential to the operation of these services and in order to obtain statistics regarding usage of these services. We do not use them to store personal information or to track an individual's usage of these services. However, you may restrict, block or delete any cookies if you prefer but this could result in the loss of functionality and may diminish your user experience. If you wish to change the usage of these cookies, please consult the help information of your web browser. Please be aware that you may have limited control over browser settings on any College provided IT equipment. Accessing these online services is your acceptance to the use of these cookies.

Please note that we are not responsible for any external services or

websites, which may have their own cookie use and policies which we have no control over.

9. **Internet use**

Internet use should normally be appropriate to staff in their work activity. Reasonable private use of the Internet is acceptable during breaks in the working day and should not interfere with performance of work related activities.

Sites and materials accessed must be appropriate for the College environment. Any sites deliberately visited that are inappropriate will be regarded as constituting a breach of the conditions of use; any inappropriate sites that are accidentally visited should be closed immediately and the user IT Services Team informed via the IT Helpdesk.

Use of the College network for gambling, political purposes, advertising or running a personal business is forbidden.

Internet access at the College is provided by the Joint Academic Network. Users agree to abide by JANETS acceptable use policy. (http://www.ja.net/company/policies/aup.html)

10. **Online resources**

The College subscribes to a number of online products and services provided by other companies; in order to make use of these, you must agree to follow the legal terms and conditions attached to each of them.

If you are given a username or password to access a certain resource, this is for your personal use only while you are a member of the College.

Many of the services the College subscribes to allow users to download and/or print material for your educational use. The College is required to emphasise that the publishers of certain services, including but not limited to the IEEE Xplore Digital Library, expressly forbid the sharing, distribution or automated gathering of files obtained from these web-sites.

If you want to make files available to others from these more restrictive sites we ask you to use hyperlinks only.

11. **Hardware and Software Configuration**

The maintenance and administration of College Systems is undertaken by identified staff within the Computing Services department. No other member of staff is authorised to carry out

administration functions on College Systems unless authorised in writing by the Head of Computing Services. Administration functions are deemed as:-
any modifications to hardware or file servers;

installation of software applications or modification of the set-up of existing applications, whether on local hard disks or network drives;

adding users, modifying folder/directory structures or login scripts and start-up configurations;

The exceptions to this rule are that users may create and change their own directory structure within their own login home or working directory, or within their Team/Faculty folder;

Users must not move hardware, disconnect network cables or modify the hardware or software configuration of their team computer systems, without permission or authorisation from a relevant manager;

Any accidental modifications or other problems with hardware and software must be reported to the IT Helpdesk immediately.

12. **Resources borrowed from the Learning Resource Centres**

The College offers members of staff the loan of certain resources from the Learning Resource Centres at each campus.

If you make use of this offer you will be required to return the resource borrowed in accordance with the loan terms set down when you initially took out the item (e.g. a laptop should be returned the same day).

In addition you will be expected to reimburse the College if these are lost or damaged at any time. In this circumstance, please contact the Learning Resource Centre Coordinator at one of the campuses for further details.

13. **System Security**

To preserve security of College systems, users are required to change their passwords at regular intervals. Users should choose a password that is easy to remember but difficult for someone else to guess.

Passwords should be a combination of letters and numbers or a word that would not be found in a dictionary. Obscenities, swear words and names, particularly of the user or people connected with them, must not be used;

Under no circumstances must users divulge their password to anyone other than a member of IT Services Team in order to find a fault. Once the fault is corrected the user should immediately change their password.

Staff should under no circumstances allow a student to log in or use any College System under their staff ID. Providing a student with access to a staff account or system will result in formal Disciplinary action in accordance with College procedure.

The exception to this rule is providing students with supervised access to electronic whiteboards or working with students on a staff machine to complete College documentation. In these circumstances students must be continuously supervised and on no occasion left alone with access to the staff network.

When leaving a computer logged in users must “lock” the machine using CTRL+ALT+DELETE on all occasions.

Students may not have any access to any staff College systems without the written permission of the Head of IT Services or Executive Director Planning and Resources.

Any attempt to bypass or disable College security systems and processes is a serious matter and which will result in disciplinary action.

14. **Software Piracy and Copyright**

All software licenses and files stored on College Systems remain the property of South Essex College and may not be copied or reproduced for non-College use without express permission from the Executive Director Planning and Resources.

All licensed software is subject to stringent legal protection and conditions of use. Breaching these legal conditions by transferring and/or copying the software will lead to disciplinary procedures.

Installation of unauthorised software on the College network is a serious breach of security and potentially places the individual and the College at risk of prosecution. Installation of unauthorised software to College systems is a serious matter and will result in disciplinary action.

15. **Software Viruses**

The College has a site licence for anti-virus software, which must be installed and used on all relevant College systems. If there is a doubt about a device being protected, the Helpline should be contacted and asked to check the machine.

The following points must also be noted:

Any software and or files obtained from outside the college and loaded onto the College Systems must be checked for viruses. This also applies to files being downloaded from the Internet;

Deliberately introducing a virus onto any College system is illegal. Anyone intentionally passing on software viruses can be prosecuted in the criminal courts. Intentional damage to Information and Communication Systems will result in disciplinary action in accordance with College procedure.

Anthony McGarel

Deputy Principal and Chief Executive

October 2014