



Staff Internet Usage Policy

The College aims to provide you with accessible, up-to-date and reliable Information and Learning Technology (ILT) to support you in your work, research and studies.

To help ensure that we maintain this level of provision the College has established this Internet Usage Policy regarding all uses by College staff of the Internet, World Wide Web, online bulletin boards, e-mail systems via the College's *Communication Network*.

Communications Network as used in this policy shall mean any and all computers, communication systems and equipment and associated software owned or possessed by the College.

The College intends to enforce this policy, but reserves the right to change it at any time as circumstances may require. The Head of Central Services is responsible for administering this policy and should be contacted should you have any questions or comments concerning this policy.

1. The Staff Internet Usage Policy applies to any use of the Internet by staff when using the College *Communication Network*.
2. Reasonable private use of the Internet is permitted but should be kept to a minimum and should not interfere with your work. Excessive private access to the Internet during working hours may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.
3. The sites accessed by you must comply with the restrictions set out in these guidelines. Accessing inappropriate sites may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.
4. In using the Internet resources at College, staff shall not:
 - (a) Make unreasonable use of personal Internet service e-mail accounts.
 - (b) Establish using College resources a personal web site, home page or other capability to make information available for browsing or posting by persons who are not College staff or students.
 - (c) Participate in on-line:
 - gambling;
 - non-educational games; or
 - non-academic chat rooms.
 - (d) Access, download, create, transmit or store:
 - any illegal, offensive, obscene or indecent images, data or other material, or any data that may be resolved into obscene or indecent images or material;

- any material which is designed or likely to cause annoyance, offence, inconvenience or needless anxiety;
 - any defamatory or libelous material;
 - any material that infringes the copyright of another person; or
 - any unsolicited commercial or advertising material
- (e) Use the College's communications networks to download or distribute pirated or 'cracked' software or data.
- (f) Install any software on the hard disk of a computer or the college network without first obtaining permission to do so from the Technical Services Co-ordinator. This includes, but is not limited to, screensavers, 'wallpaper', software updates (both manually installed and automatically downloaded and self-installing), file un-packers (e.g. PKZip, Winzip, Winrar etc), freeware and shareware.
- (g) Download software and upgrades, fixes and 'plug-ins' for any software. The exception to this is staff in Technical Services, who may download software and upgrades, fixes and 'plug-ins' for software used by the College in order to improve the College facilities.
- (h) Copy, or attempt to copy, any College software for private use.
- (i) Deliberately introduce or propagate any virus, worm, Trojan Horse, trap-door or other harmful or nuisance program or file into the college communications network.
- (j) Access, download, transmit or store information or materials owned by another party that are protected by copyright, trade secret or other intellectual property rights without the proper consent of the owner of such rights. A copy of such consent should be forwarded to the Head of the Learning Centre. Copyright applies to all text, pictures, video and sound.
- (k) Harass, demean or defame any person, including, without limitation, sexually harass, discriminate against or defame any person upon that person's race, gender, disability, sexual orientation, age, ethnicity or religious beliefs.
- (l) Access or transmit any confidential, proprietary or trade secret information of the College including, without limitation, information concerning the College's finances and business operations without prior written consent of a the Principal. A copy of such consent should be lodged with the Head of Central Services.
- (m) Express any political or religious information, views or opinion in contravention of the College's Equal Opportunities & Diversity policy.
- (n) Broadcast any information to bulletin boards or public newsgroups or persons that are not directly associated with the College.
- (o) Become a member or associate with any non-work related chat group, newsgroup or audio conference facility etc.
- (p) Conduct, or solicit or use the College communication networks for work you perform outside work/studies associated with College (for example, but not limited to, political causes, personal, religious, charitable or other commercial ventures) without prior written consent from a member of the Senior Management Team.

- (q) Interfere with in any manner or perform an unauthorised access of the College's, any other company's or any person's hardware, software or data.
- (r) Use the College Internet facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of others.
- (s) Enter the College, its staff or students into any financial obligations through the use of the Internet. The exception to this is purchases on behalf of the College made in accordance with the College's Financial Regulations.
- (t) Use the college communications network to sign up with websites or organizations that offer rewards, monetary or otherwise (e.g. Beenz), for surfing the Internet.
- (u) For reasons of security, make their password known to anyone else.

The above list of prohibited actions is by way of an example only and is not intended to be exhaustive. In any access or use of the Internet, you are expected to act in a professional, businesslike and ethical manner and remember at all times that you are a representative of the College.

5. At any time, the College at its sole discretion, can access, restrict access to, modify or remove, either permanently or temporarily, any information that staff have downloaded using the Communication Network and equipment of the College.
6. At any time, the College at its sole discretion, reserves the right to monitor Internet access by staff using the College's Communication network and equipment.
7. Access to the Internet shall be via College Communication network. Desktop modem dial-in connection to the Internet is strictly forbidden, except where prior written approval has been obtained from either the Technical Services Co-ordinator or a member of the Senior Management Team.
8. The use of the Internet by staff must strictly conform to the policies contained within the College Information Security Manual and must not hinder or interfere in any manner with the duties of their job and responsibilities to the College.
9. Any violation of this policy may result in disciplinary action, including, in appropriate circumstances, dismissal.
10. Any violation of this policy may also be subject to penalties under criminal or civil law (for example, but not limited to, Data Protection Act 1998, Copyright, Designs & Patents Act 1988, Computer Misuse Act 1990) and such law may be invoked by the college.

Members of staff may not access the Internet via the College's Communication Network at any time, through any device, unless they have read this policy and confirmed in writing that they agree to the terms and conditions contained therein.