Don’t understand?
servicedesk@ccn.ac.uk

Use of IT on all sites is closely monitored

Keep your IT account secure

Backup your USB devices and keep them safe or use 365 Onedrive instead

Don’t access or display offensive material

Regularly scan your devices for viruses or malware

Don’t disconnect or move IT equipment

Stay within the law and stay safe

Student IT Acceptable Usage Policy

This policy applies to all student users of all Information Technology (IT) systems belonging to the College, regardless of location.

This includes; networked, wireless, stand-alone and portable systems including those that connect remotely, to or through, College systems. They also apply to use of Video, Voice and Telephone systems and to audio visual equipment.

Please note that the use of all systems, including Internet, email and printing is closely monitored. The College does not actively monitor content but may use automatic tools to scan for inappropriate email and Internet content. The College reserves the right to examine any files stored on College equipment and any information being transmitted over College networks. All monitoring is compliant with the Human Rights Act 1998 and is subject to the Regulation of Investigatory Powers Act 2000.

The College monitors the use of all IT

What is monitored?

All Web content is carefully monitored to ensure that nobody is trying to access inappropriate material. The filters block some but log all pages accessed and provide a detailed record of all Internet activity onsite by user account, whether wireless or from a College PC. Other tools may be used to scan email or other content for inappropriate messages or words. Alerts will be generated where access to inappropriate material is attempted and appropriate action will be taken by the college.

Your Logon

Every student is automatically generated a unique logon account when they first enrol on a course at the College, this includes file space, email and access to the correct resources and software to succeed on your course. Your logon details and password are on your Learner Agreement or may be delivered to you via online or email services. Use of your logon is subject to this acceptable usage policy.

Key messages:

Never let anyone know your password or let anyone else log on using your account. You are responsible for the security of your account and the files stored therein.

Users will be held responsible for any misuse attributed to their account; this could include misuse by other people.

Logoff whenever you finish using the network. Make sure you return to the logon screen. If you don't, someone could modify or delete your files, or commit an offence using your account. Never leave a machine unattended while still logged onto the network.

Do not attempt to gain access to someone else's account, or data. This is a criminal offence under the Computer Misuse Act 1990.

Do not store data on local hard drives (usually C:). Machine rebuilds will remove all data on the disc. Local drives are also available to other users and therefore not secure. Store data on network drives where possible or within Office 365 Onedrive. College networks are backed up regularly therefore damaged or deleted data can usually be recovered.

Remember to backup USB device data and be careful not to leave them behind.

Report any suspected security breaches to IT Services immediately.

You must keep your logon account secret

Unacceptable Use

Student users of College IT systems (including telephones) must not cause any of the following material to be transmitted over the College, national or public networks (wired or wireless), or cause such to be stored in, printed, or displayed, on College IT systems or equipment:

- Obscene, pornographic, discriminatory, defamatory or other material that may offend
- Material that infringes a right or inherent right of another person
- Material that is designed or likely to cause annoyance, inconvenience or needless anxiety
- Material that is designed to be extremist or to radicalise

The College does not tolerate harassment in any form whatsoever. Any inappropriate material received which may cause offence to others must be reported to IT Services management immediately.

The College provides students with access to a variety of IT systems and communications media for the purposes of learning and learning support. Excessive exploitation of these facilities for personal or leisure use is not permitted.

Social networking and other leisure use is permitted within the Social Networking Zones of the Information Store. Classroom use of Social Networking is only permitted as a directed learning activity at the discretion of your lecturer. You are welcome to use your own wireless enabled devices on the College wireless network for leisure use and social networking outside of your timetabled learning activity.

The playing or storage of games on College IT equipment is only permitted for learning purposes and under direct supervision of a teacher.

Intentional or accidental damage, or disruption, to systems or data caused by *hacking* will not be tolerated and may be a criminal offence.

The College uses Internet filtering software to monitor and reduce the risk of accidental or deliberate exposure to offensive or extreme material. None of the filtering systems available are 100% effective. Therefore if you accidentally gain access to potentially offensive material, or feel that you have been barred from accessing a legitimate site, please report the incident to IT Services.

What sort of sites are blocked?

The web filters will block access to categories of sites which promote or display material inappropriate for the age groups of our students; including pornography, gambling,

terrorism, radicalisation, intolerance, personal weapons, gore and plagiarism amongst others. Alerts will be generated for some of these categories; for example where a student is attempting to access extremist or terrorist materials.

Pornography or material that might offend someone else must not be accessed or displayed. (E.g. glamour photos and horror or gore pictures)

Responsible behaviour

All users are expected to behave in a responsible manner respecting the rights and needs of other users. Personal entertainment systems should be used in a manner that does not disturb other users and general noise should be kept to a minimum, especially in open access environments.

Take care if drinking when using PCs and avoid eating altogether.

All users are expected to take care not to introduce a virus infection to College systems. Make sure you check your USB devices and never distribute unchecked files to other users. If you require assistance with virus checking then ask at the IT Services Helpdesk. Report any suspected virus infection to the IT Services Helpdesk (servicedesk@ccn.ac.uk) immediately.

The College is a responsible user of technology and is committed to sustainable IT throughout its lifecycle. Whilst we have introduced shutdown and power management utilities for our PCs, we ask that you shutdown your PC when you have finished using it.

Moving or disconnecting equipment

IT equipment should not be moved as network cables can easily be damaged and Health and Safety regulations may be breached, putting you or someone else in danger. If you need a machine moved, ask at the IT Services Helpdesk.

Network cables, mice, keyboards, monitors, audio visual equipment and other devices should not be disconnected as this can damage the connectors.

Hardware/Software downloading or installation

Software must not be installed on College IT systems except by, or in arrangement with, IT Services. Installation can only proceed once documentary evidence of software licensing has been obtained.

"Software" means any program, utility, plug-in, app, shareware or copyright dataset available from any source including the Internet ‘app stores’, USB drive or other source.

Hardware must not be installed on the College network or computers except by, or in arrangement with, IT Services. USB devices (such as flash drives, phones, iPods or tablets) are permitted if no driver installs are required.

Downloading of software (e.g. freeware, patches, drivers, movies, graphics, music, ringtones, zipped files and other files not integrated into a web page) and other licensed code, for personal use is permitted provided it goes straight to Onedrive, pen drive or other personal storage and in no way poses a threat to College systems or breaches copyright.

Please do not attempt to install software on College computers.

Copyright and Licensing

All software in use at the College must be licensed with copies of the licences lodged with IT Services for possible audit by software theft agencies. If you are using shareware or freeware from a memory stick then make sure that it's permitted for educational use.

Most local and networked software is licensed for use at the College only; copying this software is a criminal offence.

Nothing should be downloaded from the Internet for use within the College unless express permission to do so is stated by the material owner. If you are in any doubt about this you must discuss it with IT Services Management before downloading the material.

Music, film and other downloads must all be licensed for free distribution if downloaded on the College Internet links.

Communications

Whether email, blogging or social networking, personal opinions should be represented as your own and not those of the College.

Any data leaving the College should be certified virus free by the sender using the virus checking utilities on the network. Contact the IT Services Helpdesk if you require assistance.

Mail or other communications should not be sent to those who do not, or may not, wish to receive it. Use of email to send unsolicited email (SPAM) to other users may result in the loss of your email account.

Offensive material should never be transmitted through the email system.

Health & Safety

Current Health and Safety regulations and recommendations are available from the IT Services Helpdesk. They state, amongst other things, that:

"If you operate Display Screen Equipment (DSE, e.g. computer or laptop with screen & keyboard) continuously for one hour, a break of at least ten minutes should be taken. If for any reason this period is extended to two hours then the break should be of at least half an hour. In this context a break means that work away from the DSE may be undertaken; it does not mean a break away from work altogether."

All IT equipment, desks, lighting and chairs are installed to comply with current Health and Safety regulations and recommendations.

Disciplinary Procedure

All breaches of these conditions will be reported to the Principal and dealt with in line with the Prevent Duty, our Student Disciplinary Procedure and referred to the appropriate authorities as necessary.

All available evidence as well as the severity of the offence will be considered. This may result in long term to permanent loss of IT privileges or, in more serious cases, to disciplinary warnings and/or dismissal from your course and the College.

The College will be obliged to refer breaches of criminal law to the appropriate authorities.

Legal Obligations

In addition to these conditions, the use of computers in general is regulated by three Acts of Parliament: The Data Protection Act 2018 (GDPR), the Copyright, Designs and Patents Act 1988 and the Computer Misuse Act 1990. Similarly, the use of the public data telephone networks is regulated by the Telecommunications Act 1984. These and several other Acts (including the Obscene Publications Act 1978 as amended by the Criminal Justice Act 1994 and The Criminal Justice and Information Act 2008) identify a number of prohibited actions related to the use of computers.

Data about individuals may not be stored on College, or other, IT systems for any purpose unless the use of such data has been previously registered under the Data Protection Act. If you wish to hold data about individuals, contact the IT Services Helpdesk. A summary

description of the data held at City College and Paston College is registered with the Information Commissioner at http://www.ico.org.uk/

Other related College Policies (*Click to view the Policy or ask in the Library*)

Staying Safe Online Guidance for Students

Anti-Bullying and Harassment

Prevent Strategy