

Purpose

The following Computer and Internet Usage Policy has been created to minimise the risk of computer viruses and to ensure that the Institute's resources are used for their intended purpose. Failure to comply with this policy will result in disciplinary action and any costs resulting from a failure to comply will be recovered from the person(s) responsible.

Policy Statement

1. Students shall have access to the computer network designated for student use. All other Institute computers are for the use of staff members only.
2. The student computer network is for the use of current Opengate Institute students only.
3. Students use their own personal computers when they have a class.
4. Students should take great care with all computer systems of the Institute, using the computers and internet in a manner that is mature, responsible, courteous and not detrimental to others.
5. Students shall not use the computer network or internet to access or send any material that is offensive, vulgar, obscene or disrespectful. This includes images or other material of a pornographic nature, or which supports the use of restricted drugs, or which supports violence or intolerance on the grounds of race, religion and gender.
6. Students shall not use the computer network or internet to download, transfer, or store software or large files. This includes all music, video (e.g. YouTube) and program files. This includes, but is not limited to, MP3, WMA, MPEG, AVI, EXE and ISO files.
7. Students shall not attempt to access, corrupt, delete or alter any files on the Institute's computer system or network that are not the student's own.
8. Students shall not make or attempt to make unauthorised access to, or unauthorised copies of, any files on the Institute's computer system or network.
9. Students shall not remove, modify or bypass any information security mechanisms or virus prevention management systems.
10. Students shall not use the computer network or internet for commercial purposes or for personal or financial gain, including gambling or playing games.
11. Students may need computers for watching online videos.
12. The student assumes all risks for any physical or electronic damage, or viruses that may occur should a hardware device (including USB memory stick or digital camera) be connected to the Institute's computer network.
13. The Institute reserves the right to monitor its computer network at all times and carry out security audits of any systems and data, including individual user files stored on the Institute's computer network.

14. Users of the Internet should be aware that the Institute makes no guarantees concerning the privacy and security of information transmitted when using the internet. Please note it is possible that third parties can read and/or intercept this information.

15. Wireless internet facilities are available on campus. The Institute does not guarantee wireless internet connectivity at all times.