Information for Students on the Acceptable Use of College IT Facilities

The College network and computer equipment must not be used for any of the following:

- deliberately attempting to gain access to unauthorised or restricted areas within the College network or other locations;
- visiting, viewing, transmitting or downloading any Internet material which breaches legislation, College policies (eg. equal opportunities, bullying and harassment) or commonly accepted standards; or is likely to be offensive or indecent to reasonable people. This includes inappropriate websites including those promoting extreme Islamic or right-wing ideologies as well as material concerning the purchase of firearms;
- the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
- the download, copying or transmission to third parties the works of others without their permission (written material, images and software are protected by the laws on copyright);
- the transmission of unsolicited commercial material;
- corrupting or destroying other users data;
- violating the privacy or disrupting the work of others;
- using the network in a way that denies service to other users, for example, deliberate or reckless overloading of the network or computers;
- deliberately introducing viruses onto the College network;
- placing on the Internet any material, which incites, encourages or enables others to gain unauthorised access to the College's computer system.

In addition, you must not:

- install hardware on an individual PC;
- attach devices to an individual PC or VDI for any of the purposes above;
- subscribe to Internet services via the College network unless instructed by a tutor;
- load, install or modify software;
- encrypt data (the College will remove any encrypted data from the systems).

User Login and Password

You will be given a network login and password to use to access College IT systems including an email account and file store provided for your use. You must not disclose your password to another individual or organisation.

Monitoring

The College reserves the right, without notice, to access, listen to or read any communication you make or receive using College facilities. It will only do this for the following purposes:

- to establish the existence of facts
- to ascertain compliance with regulatory or self-regulatory practices and procedures
- to investigate or detect unauthorised use of systems
- to prevent or detect crime
- to provide practical help to prevent people from being drawn into terrorism and violent extremism
- to intercept for operational purposes, such as protecting against viruses and making routine interceptions such as forwarding e mails to correct destinations

Monitoring will only be undertaken by personnel who will be subject to security and confidentiality requirements and will be trained in Data Protection.

Misuse

Any misuse of IT facilities or breaches of this policy will be reported to your Tutor or Course Leader. If the misuse breaches the law or is reportable under relevant legislation (eg. PREVENT Duty under the Counter Terrorism Act 2015; Data Protection Laws) the College reserves the right to inform the police or relevant authority.

For more information please refer to the College’s Policy on Acceptable Use of IT Facilities; Policy on the Management and Monitoring of Electronic Communications, Internet and Telephones; Data Protection Policy and Information Security Policy; all available on the College’s Intranet and Website.

Student Ref ______________________________

Student Name ____________________________ Date ___________