COMSATS-Lancaster Dual Degree Programme

COMSATS Institute of Information Technology

Notes of Guidance on the Regulations Concerning Information Technology (IT)

The following notes relate to the general use of Information Technology (IT) facilities for students of COMSATS-Lancaster Dual Degree Program (DDP). The general regulations, procedures and codes of conduct and student discipline of COMSATS Institute of Information Technology (CIIT) also apply in the use of IT facilities. Breach of the regulation may lead to disciplinary action.

1. General use of IT facilities

The information technology resources provided by CIIT are for use in connection with the course related work. This includes (1) Use for learning purposes (2) Use in support of research activities

 Only registered COMSATS-Lancaster DDP student are allowed to enter IT Labs. In supervised Lab timing only schedule class is allowed to come to Lab

- Each student has a user name and password Logon to your own user name only
- No discussion is allowed in the lab. Always keep silence and discipline
- Store your important material in Z drive. Always take backup of your data
- Internet facility must be used for course related material only
- In case of any problem, report to system administrator. The students MUST cooperate and follow the instructions of the lab in- charge
- Eating and drinking in the computer labs are strictly prohibited.
- Students are required to be in proper dress as approved for them. In open labs after 9 pm the students are not allowed in casual dress using bath chappals, chaddar, tracksuits and joggers

The following are expressly forbidden and will, if detected, lead to disciplinary proceedings:

- Use which is indecent, offensive or threatening or which harasses another person or persons on or off the campus
- The promotion of views likely to incite political, racial, religious intolerance
- Use for private commercial purposes
- The use of services and facilities purely for recreational purposes
- The sending of frivolous email messages to large numbers of users

What shouldn't I do?

- Do not install any software on PCs. Take prior permission before installing any software
- Do not replace/change/attach personal hardware components to the lab PCs or hardware
- Don't write your password down or use any real word, birthday, make of your car, registration number or anything else likely to be identifiable as yours
- Don't attempt the following:
  - To use any computer unless you have explicit written authority to do so. Do not assume that because you can connect to a computer you are allowed to use it
  - To copy software or databases/datasets from CIIT's computer systems for your own personal use unless you have obtained written authority to do so from the owner of the information
  - To use any program or data belonging to another user unless you have explicit written authority to do so. Do not assume that because you know another user has a program or data which you wish to use that you are allowed to use it

.

- To alter computer material belonging to another user unless you have explicit written authority to do so. Do not assume that because you are aware of the existence of other users' computer material that you are authorized to alter it
- To access any data or programs relating to the administration of the university
- Computer games & chatting are strictly prohibited

2. Network and monitoring

Students should only connect to those network points that have been installed and enabled for their use. In CIIT, network administrators routinely monitors and analyses electronic communications traffic for such purposes as improving performance of the network, predicting trends, optimizing computer systems and investigating faults and anomalous functioning. Accordingly it keeps a temporary log of such communications activity within CIIT and between CIIT and external hosts. CIIT will only monitor the *content* of this activity if prima facie evidence of a breach in the IT Regulation exists.

Similarly CIIT will only search the content of the data files of students if a prima facie breach of the IT Regulation exists or if necessary during the investigation of a fault or anomalous functioning of the network or computer systems. On suspicion of a breach of the Regulation, CIIT reserves the right to remove or delete offending files, to impound a computer workstation or fileserver for investigation, and to suspend the person's access to some or all of the IT facilities.

3. Computer Misuse

It is a criminal offence to use a computer to access any computer systems, program or data which you are not authorized to access. 'Hacking' is a criminal offence and there are severe penalties for those convicted. In CIIT, computer accounts are to be used only by those registered to use them and authorized systems staff. It is a contravention of the Regulation to permit use by others.

IT facilities at CIIT must not be used for any of the following:

- The creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
- The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety
- The creation or transmission of defamatory material
- The transmission of material such that this infringes the copyright of another person
- The transmission of unsolicited commercial or advertising material to other organizations
- Deliberate unauthorized access to facilities or services accessible via CIIT's network
- Misuse of networked resources, such as introduction of "viruses". Storing installing and using key loggers or other hacking software is strictly prohibited. Hacking passwords and unauthorized access to other accounts will be considered as cyber crime and dealt with seriously. In the event of an infraction, the student account will be locked and the matter will be referred to appropriate authority
- Deliberate activities with any of the following characteristics:
  - wasting staff effort or networked resources, including time on end systems and the effort of staff involved in the support of those systems
  - corrupting or destroying other users' data
  - violating the privacy of other users
  - disrupting the work of other users
  - using IT facilities in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment)

****

.