F. University Code of Conduct for Users of Electronic Facilities

1. Objective

This Code of Conduct is to facilitate the efficient, effective, responsible and lawful use of the University's electronic facilities, thereby safeguarding the interests of all users and of the University.

2. Application

The Code applies to all users of the University's electronic facilities including staff, students and other authorized users, wherever they may be using the facilities.

The Code applies to all of the University's electronic facilities, irrespective of the college, faculty or other unit providing the facilities, and whether the facilities are located on a campus or site of the University or elsewhere.

Electronics facilities includes:

a. computer hardware (free standing computers, networked computers, time shared computers, terminals);
b. peripherals (for example, printers, scanners, mobile telephones when connecting to the network and electronic cameras when connecting to the network);
c. media (CD ROMs, disks);
d. computer software;
e. network connections;
f. operating and user manuals provided by the University whether or not they are owned by the University;

3. Authority

Where this Code refers to written authorization, that authority is vested in the chairperson of the department or the immediate head of the office concerned.

5. Prohibitions

In the Code, performance of or attempting to perform, a prohibited action will be considered a breach of the Code, whether or not the attempt was successful. Faculty, staff, students, and other authorized users should:

a. Not allow any other person to use their respective computer account.

A user will be accountable for breaches of this Code committed under his/ her account, if it is established that said user allowed his/her account to be used by another person or that said user did not take reasonable steps to safeguard the security of his/her account.

d. Not use any other person's computer account even with the owner's permission unless it is an approved group account to which one is granted access.

e. Not attempt to discover any other user's password by any means including the use of cracking programs.

h. Not introduce software (e.g. viruses) designed to disrupt or destroy programs and/or data, or in other ways sabotage the University's electronic facilities.