

1.13 CODE OF BEHAVIOR FOR USE OF COMPUTING RESOURCES and CORPORATE DATA

Classification: General

Effective Date: 01DEC03

Supersedes: 28SEP00

PREAMBLE

- 1.00 The University's computing resources have been acquired, and are allocated to individuals and groups, for specific academic and administrative purposes which advance the University's mission. This Code of Behavior applies to all users of the University's computing resources. Computing resources shall be understood to include corporate data.

POLICY

- 2.00 All users must ensure that the University's computing resources are used in an effective, ethical and lawful manner. The University expects all users to conduct themselves according to the high standards of professional ethics and behavior appropriate in an institution of higher learning.
- 3.00 As a condition of access to computing resources, a user agrees to use the computing resources solely for authorized academic, administrative purposes, and/or incidental, non-commercial personal use and agrees to assume responsibility for any unauthorized use, misuse or illegal use of these computing resources.

The Unit responsible for allocating computing resources or access to corporate data to individuals and groups¹ has a responsibility to inform users about this Policy. The Unit shall ensure that all users receive instruction on what constitutes appropriate and inappropriate use of the facilities, and on what to do if confronted by or notified of inappropriate usage.

- 4.00 The intentional use of the computing resources for any purpose other than academic, administrative, and/or incidental, non-commercial personal use, will be considered to be unauthorized.
- 5.00 Without limiting the generality of the above, some examples of unauthorized use or misuse of computing resources are:
- (a) Using computing resources for purposes other than those for which they were allocated;
 - (b) Using a computer account without authorization or providing computing resources to individuals or groups without the specific authorization of the relevant Unit Head or designate;
 - (c) Inspecting, altering, deleting, obtaining copies of, publishing, or otherwise tampering with files, programs or passwords that the individual is not authorized to access;
 - (d) Using computing resources, particularly electronic mail, web servers and bulletin boards, to send fraudulent, harassing or obscene messages;

¹ The unit immediately responsible for allocating such resources or access to data, e.g., an administrative work unit, Information Technology Services, Office of the Dean or Social Science Network and Data Services.

- (e) Developing or using programs that harass other users or that damage the software or hardware components of the computing resources and/or placing any destructive or nuisance programs, such as viruses, in the computing resources;
 - (f) Attempting to circumvent security systems on any computing resource;
 - (g) Compromising or attempting to compromise the integrity of the computing resources by accessing or attempting access or alteration of system control programs or files;
 - (h) Using unlicensed or unauthorized copies of computer software;
 - (i) Breaching the terms and conditions of a software licensing agreement to which the University is a party;
 - (j) Theft or misappropriation of computing resources, such as equipment, data, programs or time;
 - (k) Engaging in any action which unfairly denies or restricts the use of computer facilities to authorized users.
- 6.00 That proof of a Section 4.00 offense shall be at the upper end of the balance of probability scale on clear and cogent evidence.
- 7.00 The Unit Head² shall ensure that a user who has been found to have been in breach of this Policy is made aware of appeal or grievance procedures available to that user.
- 8.00 Users found to have breached this Policy are subject to the full range of University disciplinary procedures, including temporary or permanent loss of access privileges, and/or legal sanctions. Responsibility for dealing with allegations of misconduct may be assumed by a person or persons within ITS as identified by the Director of Information Technology Services, an academic official or the Head of a local computing facility. Faculty or staff have access to grievance procedures which are initiated with the Unit Head. Decisions regarding subsequent findings or sanctions imposed against students are appealable to the Dean of their faculty of registration.

² The Dean of an academic unit (or designate) or the Budget Head of an administrative unit (or delegate).