Department of Plant Agriculture Computer & Networking Policy

15 April 2003

modified 20 December 2007

This policy applies to the use of any computing workstation or networking facility, hereinafter referred to as the "System", belonging to the Department of Plant Agriculture. Workstations include, but are not limited to, personal computers, laptops, or any device which provides an interface connection between humans and computers.

By using the System all Users agree to comply with this policy. All Users will be fully responsible for any and all uses of their access and accounts.

1. Acceptable Use

The use of the System is a privilege granted to students, staff, faculty and sponsored visitors in support of research, instructional, administrative, and intellectual pursuits consistent with the Department's mission statement (http://www.plant.uoguelph.ca/welcome/chair/chair.htm). Users should consider University and community standards when trying to determine if an activity is appropriate.

As a condition of accessing a Departmental workstation, accessing the Department's networking facilities, and of holding a Department Local Area Network (LAN) account, the User agrees

1.1 To adhere to the University of Guelph's "Acceptable Use Policy" which can be reviewed at: http://www.uoguelph.ca/web/aupg.shtml

1.2 To adhere to the Department's "Computer and Networking Policy", which can be reviewed at: www.plant.uoguelph.ca/policy/computer-policy.html

1.3 That computer and network account(s) is/are the User's responsibility to keep secure and are provided for the User's use only. The account and any use of the account is the User's complete responsibility. User's are not to: 1) lend their account to others; 2) use passwords that are easily guessed; 3) leave passwords exposed so that others can view them; 4) remained logged in at an unattended workstation that is freely accessible to others; or 5) perform or fail to perform any action which allows others to access their account.

1.4 To not make copies of installed proprietary software or to use illegal copies of proprietary software.

1.5 Not to disable, circumvent, run programs, or perform actions that would intentionally compromise security systems, including virus protection systems.

2. Proprietary Software

2.1 Proprietary software and files installed on Departmental workstations must adhere to the license issued by the copyright holder.

2.2 Any proprietary software that is found on workstations that are owned or managed by the Department will be deleted unless the original disks, site licenses, or letter of permission are on file with the Departmental Network Administrator.

2.3 Any proprietary software detected to be in violation of licenses issued by the copyright holder that is found on workstations that are not owned by the department, but are used to access the Department System, will be reported to the Director of Computing and Communication Services (CCS) who will then undertake the appropriate action.

3. Authorization for Examination

3.1 The User agrees that the Department Chair or his/her designate, may authorize the examination of, at any time without notice, all proprietary system and proprietary application programs associated with all Departmental workstations and all Non-Departmental workstations that are used to access the Department networking facilities for compliance with the usage license of the owner. Changes in applications or new functions may result in non-departmental material, that resides on the disks, being accessed. No personal data will be consciously examined or used.

3.2 The User agrees that the Department Chair or his/her designate, may authorize the examination for, and removal of, malicious code from all files and directories, at any time without notice, within all Departmental workstations and all Non-Departmental workstations that are used to access the Department networking facilities. Malicious code includes, but is not limited to, viruses, scripts, permission changes, hacking tools, and password files.

3.3 On a case by case basis, the Department Chair or his/her designate, in agreement with the Dean of OAC, may authorize appropriate access to data files that are deemed essential to the department. This authorization will be restricted to data files that are essential to the department; no personal data will be consciously examined or used.

4. Expiration of Accounts

4.1 Department LAN accounts and access to Department workstations and networking facilities for graduate students will expire two months following the end of the last registered semester. Department LAN accounts and access to Department workstations and networking facilities for all other users will expire immediately upon termination of employment within the Department. Extension of an LAN account and access to the Department System beyond the normal expiration date will require prior application and approval by the Department Chair or his/her designate.

4.2 The termination process and other information concerning University Central accounts are found at:

http://www.uoguelph.ca/ccs/accounts/central/getting_started.shtml
http://www.uoguelph.ca/ccs/accounts/central/facstaff.shtml
http://www.uoguelph.ca/ccs/accounts/central/graduate.shtml

Notable portion of grad page:

If you have not graduated and do not register for 500 days (4 consecutive semesters) and you are not on a leave of absence, your account will be deleted. You will be notified by email with sufficient time to respond before your account is deleted.

Students who withdraw voluntarily or whose programs are terminated due to unauthorized absence will have their Central Login Account deleted 500 days (4 consecutive semesters) after the termination/withdraw date.

Students who are required to withdraw from their program will have their Central Login Account deleted 500 days (4 consecutive semesters) after the required to withdraw date.
Students attending the University of Guelph on a Letter of Permission will have their account deleted at the end of the attending semester.

“If you do NOT register during any fall or winter semester, your (University Central) account will be deleted two weeks after the final course add date... New accounts created in the fall that have NOT been validated (login with telnet general.uoguelph.ca) by the 14th day after start of the fall semester will also be deleted.”

4.3 Access to the System will be terminated for Users that are in arrears for payment of Departmental System printing charges.

5. User responsibilities

5.1 Users are not to connect a computer to the Department System without first receiving authorization to do so from the Department's Information Technology Technician.

5.2 Users are responsible for backing up their own data and information files. A number of CD writers and Zip drives are available in the Department for this purpose.

5.3 No food, drink, or loud music is permitted in the Department's computer laboratories.

5.4 Users are responsible for cleaning up after themselves in order to maintain a clean and pleasant working environment in the Department's computer laboratories.

6. Complaint and Violation Resolution Process

6.1 Violations or suspected violations of the Department's Computing and Networking Policy are to be reported without delay to the Chair or his/her designate. Issues specific to the Departmental policy will be addressed by the Chair or his/her designate. Issues involving criminal activity or violation of the University's Acceptable Use Policy will be immediately referred to the Director of Computing and Communication Services who will then undertake the appropriate action.

6.2 The Chair will initiate an investigation concerning suspected violations of the Department's Computing and Networking Policy. If, in the opinion of the Chair, the integrity or security of the System (including User services and data) is at risk, the Chair may take interim actions to protect the System. Such actions may include, but are not limited to, the locking of accounts and locking of access points during the investigation. This investigation may also involve the Director of Computing and Communication Services.

6.3 As a result of the investigation, the Chair will take one or more of the following actions:

A) If the Chair finds no evidence of a violation of the Department's Computing and Networking Policy, then no action will be taken.

B) If the Chair determines there has been a violation of the Department's Computing and Networking Policy but the offence is not serious, then the User will be informed of the decision and directed to discontinue the activities that have been deemed to violate the Policy.

C) If the Chair determines there has been a violation of the Department's Computing and Networking Policy and that the offence is serious, or if there is a pattern of repeated misuse, or if the User refuses to comply as directed in 6.3(B), then the User's Department LAN accounts and access to the Department System will be terminated.

6.4. The User may appeal a decision to terminate their access to the System as outlined in 6.3(C) to the Executive Committee, Department of Plant Agriculture.