

Department of Biological Sciences Computer Usage Policy

I. Introduction

The computing environment in Biological Sciences is a valuable resource shared by faculty, students and staff. To ensure that this resource is available to everyone, it is imperative that our network and computers are used in an ethical, professional and legal manner. The goal of this document is to provide you with specific answers to questions that you may have regarding ethical issues, network usage, software licensing, and the use of personally owned equipment.

II. Confidentiality and Network Monitoring

A. Bio-IT strives to keep your files and e-mail as secure as possible. We respect the privacy of your e-mail, however it is sometimes necessary in the course of diagnosing or resolving a system problem for Bio-IT to open an e-mail message or view an e-mail header. E-mail content is always treated as confidential.

B. Occasionally, BIO-IT or ITAP (the central IT infrastructure group) may monitor our departmental networks for excessive traffic which alerts us to computers that are infected or improperly configured.

III. Copyright Law and Intellectual Property

All University, state and federal laws and guidelines regarding copyright and intellectual property must be complied with. Copyright laws must also be complied with regarding software usage and installations (see the section below on Software Licensing), music and video file-sharing. If you are unsure what constitutes intellectual property, please see the following link. http://www.purdue.edu/oop/policies/pages/teach_res_outreach/b_10.html

IV. Peer-to-Peer Networking and Copyright Law

A. Users of popular peer-to-peer music and movie sharing programs such as KaZaa, iMesh, Gnutella, BitTorrent and others need to be concerned about violating federal copyright laws. The default settings on some of these programs configure your computer to be a file-server, such that you may knowingly or unknowingly be sharing copyrightable materials without an appropriate license to do so. The University will not protect individuals in these cases. Numerous violations occur on campus every year resulting in disciplinary action.

B. Movie and music downloads also are resource intensive and can easily slow down our network rendering it unusable. Our network scanning software can identify users who are consuming large amounts of bandwidth, and if these users have no legitimate need to download movies, they may have their network access restricted or removed in addition to other disciplinary actions. Users who have a legitimate need for moving large amounts of data should contact Bio-IT to make special arrangements for doing so.

V. Software Licensing and Installations

A. The University realizes that the cost of software is a significant investment and makes a huge effort at negotiating highly subsidized volume purchases of the popular software packages used on campus. The EULA or 'end user license agreement' for these programs vary from product to product and contains provisions for the proper installation and removal of University licensed software.

B. Because the University conducts software audits at periodic intervals to assure compliance with the license agreements and copyright laws, installing personally owned software on University-owned equipment is not allowed. The department will provide staff members with the software that they need to do their job. If bootleg or improperly licensed software is found on departmental computers, it will be removed.

C. The University requires each department to be able to produce a purchasing paper trail for each software installation. Requesting software installations through Bio-IT will ensure that your software installation meets University requirements.

For a listing of the software that the University has negotiated a license agreement, see the following link.

<http://www.itap.purdue.edu/support/licensing/SiteLicense/>

For questions regarding licensing issues, send your question to: itap-licensing@purdue.edu

VI. Revocation of Computing Privileges

A. The following is a list of activities that may result in the loss of departmental computing privileges in addition to University disciplinary actions. They include but are not restricted to:

Divulging passwords, PINS or similar items to others

Using password cracking programs on computers or accounts

Using network scanning tools or scripts

Modifying e-mail headers and forging, or 'spoofing' e-mail

Stealing another person's identity

Divulging confidential information that users access in performance of their duties

Unauthorized access to other users' accounts and files

Modifying or destroying University data

Using the University networks and systems for commercial use or personal gain

Using the networks to download music or video files that violate copyright and intellectual property laws

Sending unauthorized bulk (spam) e-mail from departmental computers

Any non-work related activity that interferes with normal network performance

B. In addition to those above, the University's computer policies on e-mail, web pages and data security must be observed as well. They can be read at http://www.purdue.edu/oop/policies/pages/information_technology/info_tech.html

C. University system administrators may revoke access at any time in order to safeguard the University's resources. Such revocation may be appealed to a committee appointed by the Vice President and Chief Information Technology Officer

D. If verifiable abuse of computer systems occurs, those responsible for such abuse will be held accountable and may be subject to disciplinary action.

E. A handful of states including Indiana now require computer administrators to report incidents of finding child pornography on academic computer systems to law enforcement agencies. While any pornography on our departmental computers is inappropriate, please be aware that the penalties for possessing child pornography are unusually severe and system administrators are required to report them.

VII. E-mail, Spam and Mailing Lists

A. The section above indicates that forging e-mail is not only unethical but is illegal. In addition, sending bulk e-mail or spam from University computers may also violate federal or state laws.

B. An individual's "bilbo" email account will be turned off six months after they leave. An individual who can have their "bilbo" email forwarded to a new email address for two years after they leave, but they must notify Steve Wilson (our department network administrator) in writing that they want their email forwarded and the email address where their "bilbo" email is to be forwarded.

C. The Biology department maintains mailing lists for departmental business, announcements and activities. As faculty and staff are sensitive to receiving unsolicited e-mail, it is imperative that these lists be used only for legitimate departmental mailings. If you are in doubt about whether your mailing is appropriate, please contact Lin Reynolds in the Main Office for department email lists and for approval to use the mailing lists.

D. A formal statement of the University's e-mail policy can be found at: http://www.purdue.edu/oop/policies/pages/information_technology/email.html

VIII. Bringing in Personally Owned Computing Devices

BIO-IT makes every effort to protect our departmental computing infrastructure. If a user brings a personally owned computer into our protected environment that is infected or misconfigured, it can damage our network and infect other computers. Therefore, we request that all personally owned computers be scanned, updated and cleaned of viruses by Bio-IT staff before they are connected to our network. We will configure your computer to update itself in the future.

Revised 6/01/07