University of Natal

Proposed policy on acceptable Internet and Email use

The growing complexity of law governing the employment relationship, as well as the legal doctrine of vicarious liability, entail significant risk for any organisation that permits its members access to the Internet. The proposed policy that follows is intended to assist in managing this risk by guiding staff and students in what is acceptable and what is not. It is of the utmost importance that all members of the University community accept their role in protecting the integrity of the University's systems and ensuring the optimal use of its Internet bandwidth, both of which play a key role in the teaching, learning and research that are the University's principal objectives.

Many institutional policies deal with these issues by means of an outright ban on all private use of email and Internet facilities. The University of Natal recognizes that such policy is not appropriate in an environment in which an intrinsic culture of freedom, and the absence of sharp lines of division between professional and private life, require a looser set of regulating arrangements. The emphasis thus falls on ensuring a measure of reasonableness in private use of these facilities. Once again, it is imperative that staff and students alike play their part in ensuring that such private use is indeed reasonable and does not place any undue strain on systems that exist for the common good.

Certain kinds of use have been excluded entirely, because of the potential consequences of such use for the integrity of the employment relationship. The policy that follows is in strict compliance with current legislation and with advisories issued by the Labour Court and the CCMA.

1. The computer equipment and resources provided by the University to its staff and students remain University property at all times.
2. Such equipment and resources are intended to be used for University purposes only. To the extent that private use is permitted, this must be consistent with the terms of University policy.
3. All data that is stored on University equipment, whether such equipment be desktop PCs or University-owned server equipment, is assumed to be confidential, unless the contrary is explicitly indicated by the data owner. No such data will be subject to disclosure or scrutiny except on the instruction of Internal Audit Services. Such instruction will not be issued in the absence of reasonable suspicion or other justifiable cause.
4. The University retains the right to monitor traffic on data lines owned or leased by it.
5. Private use of University computer equipment is permitted only to the extent that such use (a) is not for personal gain, except where such use is explicitly permitted, either by the nature of the service in question (such as newsgroups that permit private advertising) or by an agreement signed between the employee

and the University; (b) does not interfere with the duties of an officer; (c) does not expose the University to any legal liability; and (d) does not impair the rights of other members of the University community.

6. The University reserves the right to restrict or otherwise control the use of any of the Internet protocols.
7. Employees and students alike have a duty not to disclose any confidential information of the University in the course of any form of network or Internet access. The nature and scope of this duty is set out more fully in the University's Information Security Policy.
8. Any act of publication by means of one of the Internet protocols that expresses a personal opinion must include an appropriate indication that such publication does not reflect the official position of the University.
9. The following practices are prohibited:
    a) Viewing, storing, downloading or forwarding images, moving images, sound files, texts or recordings that are sexually explicit or sexually suggestive, racist, harassing, intimidating or defamatory, except where there is demonstrable academic need to access or distribute such content.
    b) Hacking in any form, including attempts to gain access to restricted resources either inside or outside of the University's computer network.
    c) Impersonating another user.
    d) Damaging or deleting files of another user.
    e) Obtaining without authorisation the access codes and/or passwords of another user.
    f) Software piracy, or other infringement of intellectual property rights in digital content.
    g) The sending, whether on the internal email system or externally, of bulk unsolicited mail, commercial advertising of other businesses, mail-flooding, or excessive cross postings on Usenet newsgroups (called spam).
    h) The use of any computer resource to promote any business or enterprise, except that of the University, unless such use is explicitly permitted by an agreement between the employee and the University.
    i) Issuing of unsolicited e-mail to indicate or gain support for any political party or religious activity.
    j) Connecting a modem to the University telephone network without authorisation.
    k) Use of a PC connected to the University network without running virus detection software.

10. Violations of this policy will be handled in accordance with procedures established in the Conditions of Service or the Rules for Student Discipline.
11. Staff and students alike have a duty not to load the University's Internet connection with unnecessary private traffic.

Approved: IT Steering Committee, 27 June 2001

For consideration by: Faculty Boards

Senate

Student Rules Committee

Joint Bargaining Forum