D R A F T
Policy Proposal for Electronic Communications & Information Technology
Feb 14, 2005

It is the District's policy that the rights of academic freedom and freedom of expression apply to the use of District computing resources. The District supports a campus and computing environment open to the free expression of ideas, including unpopular points of view. The District recognizes the privacy interests of faculty and their rights of academic freedom, freedom of expression, and participatory governance. Accordingly, the District does not and shall not monitor individual usage of its computing resources, including e-mail accounts, internet usage or data created by individuals, except as provided herein.

The use of District computing resources, like the use of other District resources, is subject to legal requirements, to standards of ethical behavior as defined and refined through the ongoing shared governance process, and usage policies. Both the nature of electronic communication and the public character of District business make electronic communication inherently less private than many users anticipate. Even the most perfect computer network is not immune from hacking or efforts to compromise the integrity and security of the system. Hence, although the District strives to develop and implement safeguards to protect system integrity and security, it cannot guarantee privacy or confidentiality of data. In addition, the normal operation and maintenance of the District's computing resources require backup and caching of data and communications, logging of activity, monitoring of general usage patterns and aggregated usage data, and other such activities that are necessary to provide network services that are relatively secure.

Under **special** circumstances, the District may monitor the activity and accounts of users of District computing resources, including login sessions and the content of individual communications, with or without notice, when:

1. required by law
2. necessary to protect the integrity, security, or functionality of District or other computing resources
3. necessary or to protect the District from criminal or civil liability
4. there is sufficient and reasonable cause to believe that (a) the user has violated or is violating this policy or other District policies/procedures, including the District's policy and procedure against discrimination/harassment/retaliation or other violations of law, or (b) the use of such computing resources may reflect cause for discipline.

Except in the event of such special circumstances as documented by the Chancellor or Vice Chancellor (such as imminent system crashes, excessive network bandwidth usage, internal or external denial-of-service attacks), any monitoring or examination of individual accounts, usage, content or hardware shall not occur unless it has been approved in advance by the appropriate Vice Chancellor, with notification to the affected employee(s) unless the Vice Chancellor concludes that good cause exists to refrain from immediately notifying the employee. Good cause may exist, e.g., in the event of an ongoing investigation into misconduct; when the District has a reasonable basis to believe that disclosure could result in destruction of evidence or retaliation against other persons; or when employees are not readily available to receive notice. A joint labor-management work group augmented with representation by the Chairperson of the

ITPC or his/her designee shall serve as a resource in defining appropriate standards and procedures regarding "special circumstances" and "good cause" based on case-by-case assessment and discussion after the fact, with appropriate confidentiality afforded to the identity of the employee(s) involved.

The results of general or individual monitoring specifically authorized by this Policy may be disclosed, after review and approval by the Chancellor or Vice Chancellor,

(a) as appropriate if requested by law enforcement agencies;

(b) in disciplinary proceedings or, as relevant, in litigation; and/or

(c) as otherwise required by law.

It should be understood by all District employees and users of District computer resources that communications may be subject to the California Public Records Act, Government Code § 6250, to the same extent as they would be if made on paper.

Limitations on Use

Computing resources are provided for professional and business use and not for personal, financial or other gain. Reasonable personal use of District computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other District responsibilities, and is otherwise in compliance with this policy.