association with any organization." The implied or expressed consent of any person toward whom an act of hazing is directed is not a defense to a charge under this anti-hazing statute.

An individual is guilty of a misdemeanor if he or she:

1. Knowingly participates as an actor in any student hazing;

2. Being a student, knowingly submits to hazing and fails to report it to law enforcement or College authorities; or

3. Is present at or otherwise has direct knowledge of any student hazing and fails to report such to law enforcement or College authorities.

An organization is guilty of a misdemeanor if it:

1. Knowingly permits or condones student hazing;

2. Knowingly or negligently fails to take reasonable measures within the scope of its authority to prevent student hazing; or

3. Fails to report to law enforcement authorities any hazing reported to it by others or of which it otherwise has knowledge.

Violation of this or any other law may subject any individual student or recognized student organization to disciplinary action (See also: Standard of Conduct VI).

Incompletes

An Incomplete is a temporary notation placed on a student's transcript to indicate that the work in a course has not yet been completed and therefore a grade has not been submitted by the instructor. The assignment of Incomplete in a course may be made only with the approval of the deans in the First Year and Upperclass Deans offices in conjunction with a faculty member. Generally speaking, an Incomplete is approved when there are circumstances that are judged to be beyond reasonable control by the student. Incompletes are granted for a specific period of time, typically ending before the beginning of the next term. For more information, see the ORC and contact the First Year and Upperclass deans.

Information Technology Policy

Dartmouth College (including all undergraduate and graduate programs) is dedicated to the missions of teaching, education, research, and public service. In support of these missions, Dartmouth provides access to electronic information resources, including networks, software, and equipment, to its students, faculty, and staff.

The Dartmouth College Information Technology Policy (the "Policy") contains Dartmouth's philosophy and requirements governing student, faculty, and staff use of its information technology resources. Dartmouth College expects each member of the community to use Dartmouth's information technology resources, including connections to resources external to Dartmouth that are made possible by Dartmouth's information technology resources, responsibly, ethically, and in compliance with the Policy, relevant laws, and all contractual obligations to third parties. The use of Dartmouth's information technology resources is a privilege. If a member of the community fails to comply with this Policy or relevant laws and contractual obligations, that member's privilege to access and use Dartmouth's information technology resources may be revoked. The use of Dartmouth's information technology resources to send communications to Dartmouth or non-Dartmouth persons or entities typically identifies the sender as belonging to the Dartmouth community. Each member of the community should therefore recognize that any such communication may

reflect on how Dartmouth is perceived by not only the Dartmouth community, but also the public at large. For further information, please see the section on DND, Name Directories, User Name, and Account Revocation Procedures.

By adopting the Policy, Dartmouth recognizes that all Dartmouth students, faculty, and staff are bound not only by the Policy, but also by local, state, and federal laws relating to electronic media, copyrights, privacy, and security. Other Dartmouth policies that relate to this Policy and also apply to Dartmouth College students, faculty, and staff (collectively, the "community") include the Dartmouth College Copyright Policy, the Dartmouth College Policy and Guidelines on Copyrighted Materials, the Dartmouth College Patent Policy, the *Dartmouth College Student Handbook* and faculty handbooks, and the Dartmouth College Exempt and Non-exempt Staff Handbooks. Each member of the Dartmouth community is expected to be familiar with the relevant foregoing policies.

Freedom of Expression and Misconduct

Freedom of expression and an open environment within which to pursue scholarly inquiry and to share information are encouraged, supported, and protected at Dartmouth. (Please see the principle of "Freedom of Expression and Dissent" that appears in the Handbook of the Faculty of Arts and Sciences and the *Student Handbook*.) Censorship is not compatible with the goals of Dartmouth. While Dartmouth may limit the use of some computers or resources to specific research or teaching missions, freedom of expression will generally be protected. While Dartmouth rejects censorship, behavior that constitutes misconduct will not be protected. Such behavior includes, but is not limited to, the use of Dartmouth's information technology resources in connection with child pornography, harassment of any kind, copyright infringement, theft, unauthorized access, and other violations of the law.

To comply with federal regulations governing tax-exempt organizations, Dartmouth technology resources may not be used for mass and unsolicited communications used in connection with lobbying (except official Dartmouth activities authorized by the Office of the Provost) or political campaigns. Communications that in part may contain political information, when sent to a select few individuals and that pertain to professional and work related issues, are permissible. In addition, such resources should not be used for private business or commercial activities, except where such activities are otherwise permitted under applicable Dartmouth policies.

Privacy

Members of the Dartmouth community have reasonable expectations of privacy in their use of information resources, in accordance with this policy. State and federal law, and Dartmouth policy, prohibits unauthorized access to computer and telephone systems. No one should use aliases, nicknames, pointers, or other electronic means to capture information intended for others without permission of the intended recipient. Attempts to gain unauthorized access to machines or computer records, to decrypt encrypted materials, to monitor other individuals' computer or network use, to attempt to obtain their passwords, or to obtain privileges or information to which the user is not entitled, are prohibited.

Information stored on an individual's account is presumed to be private unless the account holder has made the information available to others. If, for example, the account holder allows public access to files via file sharing, it is presumed that the account holder has waived his or her privacy rights to those files.