

Student Technology Use Agreement

Read the text below and confirm your agreement to its terms and conditions at the bottom of the page to continue.

All users of academic computing facilities and resources are subject to the following regulations:

- University of Houston-Downtown students, faculty and staff are eligible to use academic computing facilities and resources. Access will not be granted to others without approval by the Coordinator of Computing Lab Services.
- Users must present a valid University of Houston-Downtown I.D. card before entering the Academic Computing Lab.
- Lab users are expected to conduct themselves in a responsible and courteous manner while in the Academic Computing Lab.
- Computing accounts are for use only by the person to whom the account has been issued by authorized computing personnel. A user may not disclose his/her password or allow other users to access his/her account. The accounts are intended solely for university related purposes. They are not to be used for business or other profit producing endeavors or for recreational purposes. Games are prohibited on all Academic Computing resources. This restriction does not apply to games and simulations used in conjunction with academic courses or research. The Coordinator of Computing Lab Services must receive written notice from the instructor of record in advance of such use.
- Compromising the security of any computer or network, and/or using university computing resources to engage in any illegal activity is strictly prohibited.
- Each user is fully responsible for the activity of any account that has been assigned to him/her. If a user suspects that his/her account has been accessed by another user, the Coordinator of Computing Lab Services should be notified immediately.
- Any changes to student accounts or access to any system must be requested by the responsible faculty member.
- Users may not write, use or have possession of programs that may be used to intimidate, harass, or create an offensive environment for or invade the privacy of other users.
- Users shall not represent themselves electronically as others.
- Users shall not obstruct or disrupt the use of any computing system or network by another person or entity either on the UHD campus or elsewhere.
- Users shall not by any means attempt to infiltrate a computing system or network either on the UHD campus or elsewhere.
- All users of UHD external network connections shall comply with the evolving "Acceptable Use" policies established by the external networks' governing bodies. Copies of policies relating to commonly accessed external networks will be made available in the Academic Computing Lab.
- Copying of copyrighted software is illegal and is prohibited.

- The University of Houston-Downtown forbids, under any circumstances, the unauthorized reproduction of software or use of illegally obtained software. Using university equipment to make illegal copies of software is prohibited.
- Lab users may bring licensed personal copies of software into the academic computing facilities, but may not install software on any computer or network or alter any existing software. Proof of ownership may be requested of users.
- Users should not attempt to repair any malfunctioning equipment or software, but should report any such occurrences to computing personnel.
- Smoking, eating, and drinking are not permitted in academic computing facilities.
- Reservations for general academic computing lab use are not normally required; however, a temporary reservation system will be adopted as needed.

Although Information Technology will make efforts to provide a safe and problem free computing environment, in no event will the University or the Division of Information Technology be liable for loss of data, inconvenience or other tangible or perceived damage resulting from or relating to system failures, viruses, user negligence, or other occurrences.

These regulations may be amended at any time. Use of computer accounts and resources in violation of these regulations, UHD policy, or any federal, state, or local laws may result in revocation of the individual's account privileges or suspension of access to computing resources, and may subject the account holder to university disciplinary action and/or criminal prosecution.

Examples of Misuse of Computing Resources or User Accounts

- Using a computer account that you are not authorized to use. Obtaining a password for or gaining access to a computer account or directory which has not been assigned to you by authorized computing personnel.
- Using the campus network to gain unauthorized access to any computer system.
- Knowingly performing an act, which will interfere with the normal operation of computers, terminals, peripherals, or networks; to another user, a program intended to damage or place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan horses, and worms.
- Attempting to circumvent data protection schemes or uncover security loop holes.

Violating terms of applicable software licensing agreements or copyright laws.

- Deliberately wasting computing resources (i.e. playing computer games, etc.)
- Using electronic mail or other means to harass others.
- Masking the identity of an account or machine.
- Posting on electronic bulletin boards materials that violate existing laws or University policies.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.
- Causing the display of false system messages.
- Maliciously causing system slow-downs or rendering systems inoperable.

- Changing, removing or destroying (or attempting the same) any data stored electronically without proper authorization.
- Gaining or attempting to gain access to accounts without proper authorization.
- Making copies of copyrighted or licensed software.
- Using university computers for unauthorized private or commercial purposes.

Activities will not be considered misuse when authorized by appropriate university computing officials for security or performance testing.

GatorMail Guidelines

- Use of e-mail services is governed by existing policies as described in UHD Policy Statements: Academic honesty, Regulations for Using Academic Computing Facilities and Resources, Student Rights and Responsibilities—see the Student Handbook for specific policies and additional rules and regulations regarding the use of e-mail and other computing resources.
- Students should check their e-mail on a frequent and consistent basis in order to stay current with University-related communications. Students must recognize that certain communications may be time-critical.
- To ensure the availability of e-mail service for educational purposes, the university limits the amount of storage space allocated for each student's e-mail account. Once this limit is reached, the student must delete existing messages. The university is not responsible for e-mail messages that are not delivered to the student's account if the student's e-mail account has exceeded its size limit.
- Students should exercise caution in using e-mail to communicate confidential or sensitive matters, and should not assume that e-mail is private and confidential.
- All messages and files that exist at the time an account is terminated will be deleted and cannot be recovered.
- Use of student e-mail is restricted to sending and receiving messages consistent with academic and scholarly activities. Students must properly identify themselves as originators of email messages, and refrain from using email for any purpose that is not consistent with the policies regarding the conduct of students at UHD.
- Students are responsible for the activity of any account that has been assigned to him or her. If a student suspects that another person has accessed his or her account, the Coordinator of Computing Lab Services should be notified immediately.
- Students should use restraint and observe the rules of "netiquette" in e-mail communications.
- Students shall not send messages or postings that may be used to intimidate, harass, create an offensive atmosphere, or that could be construed as abusive or offensive.
- Students shall not send messages or postings for commercial or personal gain.
- Students should not propagate chain letters (e.g., any communication which requests or demands the recipient forward the message to one or more individuals) or send the same message to multiple groups.
- Students shall not attempt to perform mass mailings to the entire campus (or a large subset of the campus).

- Students shall not deliberately alter or attempt to conceal their true identity, return mail address, or the origination location of the message.
- Students shall not deliberately set forth to interfere with the reception of e-mail by an individual.
- Student e-mail should not be used for any unlawful activity.
- Students shall not deliberately set forth to intercept or receive, and/or view another individual's e-mail without that user's consent.
- Students shall respect the laws governing the use of copyrighted, intellectual property, which includes computer software.
- Students shall not commit acts associated with denying, interfering with or disrupting service of UHD's e-mail service or that of any other agency.
- E-mail services are not to be used for any type of harassment of an individual or organization.
- UHD assigns student e-mail accounts as a means of communication between faculty, staff, and students. The use of e-mail services should be for legitimate educational purposes. The Office of the Dean of Student Affairs governs access to student e-mail services.



I agree to the terms and conditions of this agreement.