

Chaminade University

Student Email Help

[Logging In](#)

[Forwarding Mail](#)

[Changing Your Password](#)

[More Email Help Options](#) << [link to University_Email.doc](#)

All Chaminade students are given Chaminade email accounts. It is essential that you check your email frequently (at least once each day) because important messages from your instructors, university administrators, and fellow students will be sent to that address.

You can read your mail from any computer connected to the Internet which has Internet Explorer or other web browser installed. There are other ways to access Chaminade email, but we recommend that you use the web interface for your email.

Below are basic instructions for using Chaminade's email. This is a full-featured email interface, and not all features are covered below.

Logging In

1. Enter the address <http://student.chaminade.edu/> in the address bar, or use the "CUH Email" link at the bottom of every <http://www.chaminade.edu/> web page.



2. Enter your ID (firstname.lastname) and your password. Do **not** check the "Remember userID and password" box unless you are **sure** no one else will use the computer! Then click on the "Log In" button. An information screen will appear. Click "Continue" to move to the next screen.

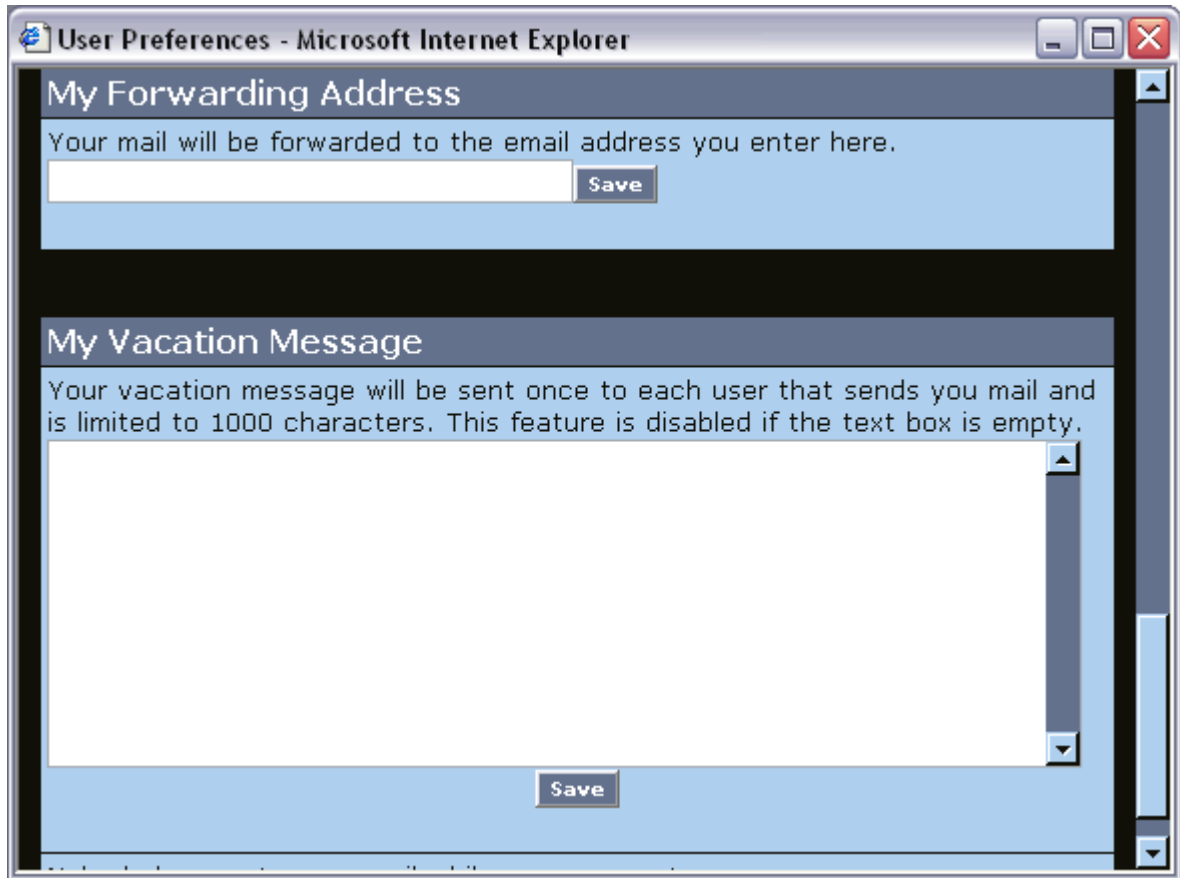
Forwarding All Mail to a Different Address

All official Chaminade email will be sent to your student.chaminade.edu address. You can forward all mail from your Chaminade account to your personal email account if you wish. *Note, however, that forwarding is performed at your own risk. You are responsible for all email sent to your Chaminade account whether you receive it at your other address or not.*

1. To forward mail, use the "Forwarding" item on the "Options and Styles" pull-down menu. **Be sure you don't have any "pop-up blockers" enabled!**



2. Enter the address you want the mail to go to in the "My Forwarding Address" box and click on "Save". A confirmation message appears. All of your mail will now go to the address you entered.



You need not put anything in the "My Vacation Message" block.

Be sure to check that your mail is actually successfully forwarded. Ask a friend to send mail to your student.chaminade.edu address and verify that you can read it at your forwarded address.

To remove forwarding, follow the same instructions, but use the delete key to remove the forwarding address and save. Your mail can now be read directly in the student.chaminade.edu account.

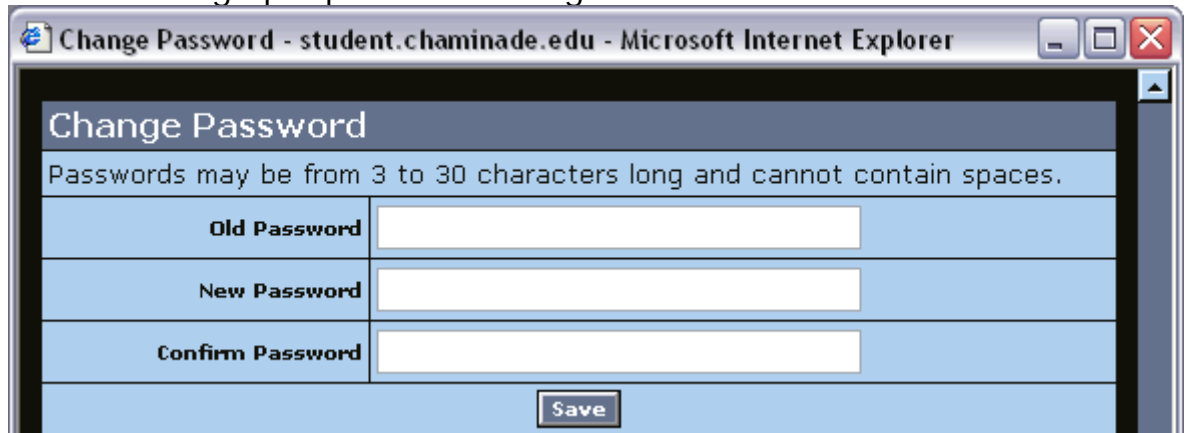
Changing Your Password

You should change your password the first time you log on, since, unless you do, anyone who knows your Social Security Number or birth date will be able to access your mail.

1. Use the same pull down menu as you did to forward mail, but select "Password." **Be sure you don't have any "pop-up blockers" enabled!**



This will bring up a password change screen.



2. Type your old password in the first field, then the new password you desire in the second and third box. The characters you type will be replaced by ***. When you are finished, click on the "Save" button. When you change your password, no one but you will know it or be able to retrieve it; don't forget it! We don't recommend you write down your password, but you might want to create a MS Word document with a hint to remind you what your password is.

*Click here to get more information on web mail.

Acceptable Use Policy for Chaminade University Technology Resources

General Statement: Chaminade University is committed to excellence in teaching. In an effort to support the University community in these endeavors, the institution has assembled a wide variety of technology resources for general use. These resources are for use by persons currently affiliated with the University, including but not limited to students, faculty, and staff.

The technology resources that are owned by the University are to be used for University-related activities for which they have been assigned. University technologies are not to be used for commercial purposes or non-University-related activities without written authorization from the University.

Access to technology resources at the University is a privilege and must be treated as such by all users. Like any other campus resources, abuse of these privileges can be a cause for campus disciplinary procedures and/or legal action. Furthermore, the University reserves the right to extend, limit, or restrict technology privileges and access to information resources. This acceptable use policy includes all provisions of the Hawai'i Revised Statutes Computer Crime Statute of the Hawai'i penal code. The University's website privacy policy is also important supplemental material to this policy. When an employee or student leaves Chaminade University, unless authorized in advance, all university privileges will be suspended immediately.

With regard to web pages hosted by the University, Information Services is available to provide stylistic assistance, although its main role is an advisory one, with primary control of content residing within each unit (see Policy Manual Vol. II Section 2.9.4.9 Suspension of Individual Privileges for further information). However, under the direction of the President's Leadership Council, Information Services will have the ultimate authority to decide if web content is acceptable and to suspend access to it if it is deemed unacceptable.

The Computer Crime Statute of the Hawai'i Revised Statutes of the Hawai'i penal code, while not reproduced here, shall be considered a part of the University's Acceptable Use Policy. The University's website privacy policy is also important supplemental material to this policy.

The University has the right and responsibility to provide the University community with information technology resources and

services. While providing these services is of primary importance, there are other areas of importance aside from physical resources. The following is a general description of the responsibilities and obligations of the users. Since certain privileges are given to each member of the University community, individuals are held accountable for their actions as a condition of continued membership in this community.

Precautions Relative to the Misuse of Technology Resources: It is imperative that all users of the University's technology resources be aware of the risks and dangers that can occur from using these resources for non-academic, non-research purposes. We strongly discourage users from using the technology resources for purposes of establishing personal contact with individuals previously unknown to the user. The possibility of the user being put in danger of physical harm, or another type of compromising position, cannot be overstated. Therefore, users are strongly urged not to use technology resources for purposes of pursuing personal relationships.

Criminal Acts: No person shall use University technology resources for illegal or criminal activities, including, but not limited to illegally accessing computer systems (this University's or other systems), exploiting security flaws, releasing computer viruses or worms, obstruction or denial of service attacks, and accessing files, including e-mail, without authorization. Any illegal and /or criminal activities will result in action up to and including all provisions of the Hawai'i Revised Statutes Computer Crime Statute of the Hawai'i penal code.

Moral and Ethical Standards: It is expected that all users of all University technology resources will be guided by the ethics, morals, and Catholic Marianist values and standards of this institution. Every user must respect the rights and dignity of others by using the technology resources responsibly and in accordance with the highest ethical and moral standards. Therefore, certain behavior not consistent with the ethics, morals, and values of this institution and/or any reasonable person will not be tolerated. The following are some, but not all, uses considered unacceptable:

Harassment that would cause distress, embarrassment, discomfort or intimidation based on race, national origin, disability, religious belief, gender, sexual orientation or other types of intimidation.

Offensive, tasteless, sexually explicit materials and images.

Using the institution's resources as a conduit to attempt unauthorized access to on or off-campus resources.

Vulgar, abusive, or offensive language.

Violation of copyright laws by using, copying, distributing or storing copyrighted programs and materials, including downloaded music and/or video data from the Internet.

Academic dishonesty, including but not limited to plagiarism (copying of the work of others in violation of authorial integrity).

Behaving in any way that demonstrates a lack of respect for the rights and privacy of others.

If anyone is witness to, or the victim of, any of the above abuses, it is that person's responsibility to report the situation to either the Director of the Office of Educational Technology (OET) or the Director of Management Information Systems (MIS), who may handle the individual situation to a satisfactory conclusion, or refer the action for disciplinary action to appropriate administrators or governing bodies.

Common Courtesy and Respect for the Rights of Others: Each person is responsible to all other members of the University community in many ways, including to respect and value the rights of privacy for all, to recognize and respect the diversity of the population and opinion in the community, to behave ethically, and to comply with all legal restrictions regarding the use of information that is the property of others.

Privacy of Information: No person should look at, copy, alter or destroy anyone else's personal files without explicit permission (unless authorized or required to do so by law or regulations). The ability to access a file or other information does not imply permission to do so. Similarly, no one should connect to a host on the network without advance permission. People and organizations link computers to the network for various reasons, and many consider unwelcome connections to be attempts to invade their privacy or compromise their security.

Intellectual Property: Each person is responsible for recognizing (attributing) and honoring the intellectual property rights of others. Violation of this is plagiarism. See Subsection 4.12.3 of Volume IV of this Policy Manual.

Harassment: No member of the community may, under any circumstances, use technology to libel, slander, or harass any other person. Persons so doing may come under the University Discipline Procedures in Volume IV, Subsection 4.8.9; Volume V, paragraph 5.8.1.4; Volume VII, Subsection 7.6.2; depending on the severity of the incident.

Examples of computer harassment:

Using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm.

Using the computer to contact another person repeatedly to harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease.

Using the computer to contact another person repeatedly regarding a matter for which one does not have legal right to communicate, once the recipient has provided reasonable notice that the recipient desires such communication to cease (such as debt collection).

Using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another.

Using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

Game Playing: Limited recreational game playing, that is not part of an authorized and assigned research or instructional activity, is tolerated within the parameters of each department's rules. Recreational game players occupying a seat in a computing facility must give up that seat when others who need to use the facility for academic or research purposes are waiting. Game playing that interferes with the operation of the University's technology resources will not be tolerated.

Commercial Use: No person shall use University technology resources for commercial purposes or private gain, including, but not limited to, marketing a home business or hosting a commercial web page.

Information Integrity: It is the user's responsibility to be aware of the potential for, and possible effects of, manipulating information, especially in electronic form, to understand the changeable nature of electronically stored information, and to verify the integrity and

completeness of information that is compiled or used. The user should not assume that information or communications are correct when it appears contrary to expectations; it should be verified with the person who originated the message or data.

Sharing of Access: Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. Each individual is responsible for the use of his or her own account, password or authorization codes. Disciplinary action may be taken against persons using passwords and/or authorization codes assigned to another user(s).