Appropriate Use & Computer Ethics Policy

Technology Usage Policies
Access to computing resources and networks that are owned or operated by the university imposes certain responsibilities and obligations, and is granted subject to university policies and applicable laws. Appropriate use is always ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment. Users are responsible for taking appropriate precautions to reduce their risk of downloading viruses or other potentially harmful software. The university is not responsible for any virus infection that is the result of accessing the Internet using university networks.

Users who access the university network using a privately-owned computer system or mobile device are responsible for adhering to the university Technology Usage Policies. This applies whether the user connects to the network directly, via a virtual private network, and/or through cloud services. Any individual who violates the Technology Usage Policies will be subject to disciplinary action. Disciplinary procedures applicable to students are found in Volume VI. Disciplinary procedures applicable to faculty are found in Volume IV. Disciplinary procedures applicable to administrators and staff are found in Volume V.

Appropriate Uses of Computing Resources
Users of the university network or computing resources must comply with all university policies including but not limited to any ethical standards or Code of Conduct that applies to that user. Unauthorized use of university resources, unauthorized access to files and data, violation of the Copyright Act, and violation of the laws of the applicable jurisdiction are strictly forbidden. Users should avoid monopolizing university resources. The bandwidth of the university network is limited and users should avoid transmitting or receiving unnecessarily large amounts of data. Users may not run servers or daemons or build their own private network on shared systems without prior permission.

The primary use of email accounts provided by the university should be related to university business and academic pursuits. Secondary uses may include personal and recreational uses that will be curtailed if they interfere with the primary function. Personal messages will be treated no differently than other messages.

Prohibited Uses of Computing Resources
In addition to adherence with the above and with all applicable university policies, users of the university network or university computing resources are explicitly forbidden from the following activities. This policy does not restrict the right to engage in actions protected by the National Labor Relations Act, including the right to discuss wages and terms and conditions of employment with co-workers and others and to take actions to protect these rights.

1. Use of another person's login name and/or password.
2. Obtaining access to the files or communications of others without proper authorization and with no substantial university business purpose.
3. Attempting to intercept any electronic communication without proper authorization.
4. Use of computer programs to decode passwords or access control information.
5. Attempt to circumvent or subvert system security measures.
6. Intentionally engaging in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, modifying or damaging files, or changing network settings.
7. Use of university systems for partisan political purposes, such as using electronic mail to circulate advertising for political candidates. However, small groups/clubs, e.g. Young Democrats or Republicans, may circulate information among themselves.

8. Use of university computing resources, including the university network, to violate state, federal, or local laws. This includes, but is not limited to, violation of the Copyright Act.

9. Use of university networks or email accounts provided by the university to harass, intimidate, or otherwise interfere with the ability of others to conduct university business and academic pursuits. This includes sending unsolicited and unauthorized mass mailings.

10. Use of the university’s systems for personal gain; for example, by selling access to your login name and password or by performing work for profit in a manner not authorized by the university.

**Copyright Policy**
The university expects all users to comply with the applicable laws governing copyrighted digital material. It is the intent of Caldwell University to inform students about copyright law and campus policies related to violating copyright law as well as civil and criminal penalties for unauthorized distribution of copyrighted materials. Violators of the Copyright Policy are subject to disciplinary action. Sanctions may include suspension of access to University networks. The university will periodically review this policy to ensure effectiveness.

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or “statutory” damages affixed at not less than $750 and not more than $30,000 per work infringed. For “Willful infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys’ fees. For details, see Title 17, United States Code, Sections 504, 505. Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. For more information, please see the website of the U.S. Copyright Office at [www.copyright.gov](http://www.copyright.gov).

EDUCAUSE provides a comprehensive list of legal downloading resources on its website at http://www.educause.edu/legalcontent. Users are directed to this website for links to appropriate sites. The university employs technology based deterrents in compliance with the Higher Education Opportunity Act of 2008. This includes accepting and responding to DMCA notices. To report any suspected electronic copyright infringement originating at Caldwell University, please contact the designated agent (per the DMCA) listed below:

Donald O’Hagan
Chief Information Officer
Caldwell University
120 Bloomfield Avenue
Caldwell, NJ 07006
973-618-3759
DOHagan@caldwell.edu

**The Electronic Communications Privacy Act**
In 1986, Congress passed the Electronic Communications Privacy Act (ECPA) that made it illegal to intercept electronic communications on a public or private network without proper authorization. The
ECPA provides electronic transmission of messages the same privacy protection as telephone calls over the public telephone systems. System operators are not permitted to divulge the contents of messages except under a narrow set of circumstances. The ECPA also protects internal systems, such as those at Caldwell University, from unauthorized interception of messages by outside sources. However, the ECPA permits messages that are stored on internal systems to be accessed by authorized personnel without violating the Act. This statement sets forth the university's policy with regard to the use of, access to, and disclosure of electronic communications. For purposes of this policy statement, electronic communications includes but is not limited to electronic mail, Internet services, voice mail, audio and video conferencing, and facsimile messages that are sent or received by faculty, staff, students, and other authorized users of university resources.

**Monitoring Network Use**
The university will not monitor the contents of electronic communications as a routine matter. However, under certain circumstances the university reserves the right to access such information to the extent permissible by law. This includes, but is not limited to, when such access is required by law or court order, necessary to identify or diagnose security vulnerabilities, to preserve public health and safety, to carry out essential business functions of the university, or when there are reasonable grounds to believe that a violation of law or a significant breach of university policy may have taken place. Such monitoring is a serious matter, and university will only do so with explicit authorization. For the faculty, appropriate authorization is the Vice President of Academic Affairs and the President of the Faculty Council. For the staff, appropriate authorization is the Vice President for Institutional Effectiveness. For the students, appropriate authorization is the Vice President of Student Life. This policy applies to all use of university networks, including Internet access and use of e-mail.

The university retains the right to employ appropriate network traffic and bandwidth analysis methods.