

Cornerstone University

Policy on Responsible Use of DiscipleNET Resources

Approved: January 1, 2004

1.0 Overview

Cornerstone University provides students and employees with access to network, computing and other technological resources as an integral part of the educational and work environment. Those using these resources should do so responsibly in a manner consistent with the University mission and objectives. As a private network, the University reserves the right to define and enforce appropriate regulations to ensure that the use of these resources is consistent with its mission. This policy serves to explicate the expectations of responsible use, the norms for DiscipleNET monitoring and administration, and the enforcement mechanisms to ensure compliance.

The purpose for publishing a responsible use policy is not to impose restrictions that are contrary to Cornerstone University's established culture of openness, trust and integrity. The University desires to protect its students, employees, and partners from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective information security and responsible use is a community effort involving the participation and support of every Cornerstone University student, employee, and other affiliates who interact with information and/or information systems. It is the responsibility of every DiscipleNET client to know this policy and to conduct his or her activities accordingly.

2.0 Scope

This policy applies to all equipment and communication facilities that are owned or leased by Cornerstone University and/or is connected to the network of Cornerstone University. This policy applies to all students, employees, contractors, consultants, temporaries, and other workers at Cornerstone University, including all personnel affiliated with third parties as they conduct business with the University. Unless otherwise designated, all policy statements apply to all clients of DiscipleNET at all times.

3.0 Authority

This policy is approved and adopted by the Chief Information Officer (CIO) of Cornerstone University based upon the delegated authority granted to the CIO by the President of the University.

4.0 Policy Definitions

- 4.1 Cornerstone University – aka, the University, refers to the corporation as a whole and/or any sub-entity thereof
- 4.2 DiscipleNET – the totality of all computing and information assets of Cornerstone University and/or any subcomponents thereof
- 4.3 Information Assets – any and/or the totality of all data and information under Cornerstone University control and for which Cornerstone University is responsible to protect
- 4.4 Technology Asset – any and/or the totality of all equipment and/or operating software use to input, manipulate, process, transmit, and/or display information assets that is owned, leased, or operated by any client of Cornerstone University
- 4.5 Client – Anyone who uses any information and/or technology asset of Cornerstone University, including, but not limited to, students, employees, contractors, consultants, temporaries, and other workers at Cornerstone University, including all personnel affiliated with third parties as they conduct business with the University

5.0 Basic Principles

The use of DiscipleNET resources are for the educational and administrative functions necessary to conduct the mission and business of Cornerstone University. Ethical standards which apply to other University activities (e.g., discernment policies, contractual obligations, and all local, state, and federal regulations and laws) apply equally to the use of DiscipleNET resources. As in all aspects of University life, DiscipleNET clients should act honorably and in a manner consistent with ordinary ethical obligations. Stealing, deception, vandalism, poor stewardship, and harassment are just as wrong in the context of DiscipleNET as they are in all other domains of the University.

As stewards of the technology and information entrusted to the University, the following principles are to be upheld.

- Respect one another's need for access to DiscipleNET and act in a manner that allows all clients to flourish in the use of these resources.
- Do not waste DiscipleNET resources.
- Do not destroy DiscipleNET resources either through neglect or purposeful acts.
- Communicate with respect and integrity.
- Respect other's tangible and intellectual property.
- Respect other's privacy.

Use of DiscipleNET is restricted to authorized clients. For the purpose of this policy, an authorized client is an individual who has been granted specific access privileges by an authorized agent. Generally speaking, access privileges are controlled via login ID's and authentication mechanisms, e.g. passwords. Individual clients are responsible and accountable for the proper use of their access privileges, including protection of their login IDs and passwords. Clients are responsible for reporting any activities that they believe to be in violation of this policy to Information Systems.

6.0 Policy

6.1 General Use and Ownership

- 6.1.1 Passwords, codes and the contents stored on any DiscipleNET asset, including, but not limited to, network, computer, telephone and voicemail systems are the property of Cornerstone University.
- 6.1.2 While Cornerstone University desires to provide a reasonable level of privacy, clients should be aware that the data they create on DiscipleNET remains the property of Cornerstone University unless otherwise governed by other University policy. Because of the need to protect and monitor DiscipleNET, a guarantee of the confidentiality of information stored on any technology asset cannot be made.
- 6.1.3 Clients are responsible for exercising good judgment regarding the reasonableness of personal use of DiscipleNET assets.
- 6.1.4 Final determination of responsible use by any client of any DiscipleNET resources lies solely with the Chief Information Officer.
- 6.1.5 For security and network maintenance purposes, authorized individuals within Cornerstone University may monitor equipment, systems, network traffic and data at any time per Information Systems policies.
- 6.1.6 Cornerstone University reserves the right to audit networks, systems and data to ensure compliance with this policy and in response to official investigations.

6.2 Security and Proprietary Information

- 6.2.1 The user interface for information contained on any DiscipleNET system should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines. Examples of confidential information categories include but are not limited to: private University communiqué, University strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Clients should take all necessary steps to prevent unauthorized access to this information.
- 6.2.2 Login IDs and passwords are to be kept secured and may not be shared. Authorized clients are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly and user level passwords should be changed every six months.
- 6.2.3 All PC's, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.
- 6.2.4 Because information contained on portable computers is especially vulnerable, special care should be exercised to secure these devices.
- 6.2.5 Postings by clients, especially by employees, from a Cornerstone University email address to newsgroups, listservs, discussion forums, etc., should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Cornerstone University, unless posting is in the course of official business duties.

- 6.2.6 No computer may be connected to DiscipleNET with the written consent of the Director of Network Operations of the Chief Information Officer.
- 6.2.7 All hosts used by clients that are connected to the Cornerstone University network, whether owned by the client or Cornerstone University, shall be continually executing approved virus-scanning software with a current virus database. Clients may not override virus scanning software that is installed by Information Systems staff.
- 6.2.8 Clients must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

6.3 Unacceptable Use

- 6.3.1 The following activities are generally prohibited unless expressly exempted from these restrictions during the course of legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). The lists below, while not exhaustive, attempt to provide a framework for activities which fall into the category of unacceptable use. Final determination of acceptable and unacceptable use lies within the authority of the Chief Information Officer.

6.3.1.1 System and Network Activities

The following activities are strictly prohibited, without exception:

1. Under no circumstance is a client utilizing a DiscipleNET asset authorized to engage in any activity that is illegal under local, state, federal or international law.
2. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by Cornerstone University.
3. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Cornerstone University or the client does not have an active license is strictly prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Willful introduction of malicious programs into DiscipleNET (e.g., viruses, worms, Trojan Horses, e-mail bombs, etc.) or any other network or server.

6. Revealing any DiscipleNET account ID and/or password to others or allowing the use of your account by others. This includes family and other household members when work is being done at home.
7. Using a DiscipleNET asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the client's local jurisdiction.
8. Using a DiscipleNET asset to create and/or distribute defamatory or threatening communications.
9. Using a DiscipleNET computing asset to access, create, or distribute any obscene, sexually explicit or pornographic materials.
10. Making fraudulent offers of products, items, or services originating from any DiscipleNET asset.
11. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
12. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the client is not an intended recipient or logging into a DiscipleNET asset that the client is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service attacks, and forged routing information for malicious purposes.
13. Port scanning or security scanning unless prior permission by the Chief Information Officer is secured.
14. Executing any form of network monitoring which will intercept data not intended for the client's host, unless this activity is part of an employee's normal job/duty.
15. Circumventing user authentication or security of any DiscipleNET asset.
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a client's terminal session, via any means, locally or via the network.
17. Intentionally creating, modifying, reading, accessing, or copying data to or from any areas to which the client has not been granted access. This includes accessing, copying, or modifying the files of others without their explicit permission unless this is done as part of system administration by authorized employees.

18. The establishment of any function that provides unauthorized access, via the Internet connection or otherwise, to any DiscipleNET asset without the express written permission of the Chief Information Officer. This includes peer-to-peer applications that bypass normal network authentication protocols.
19. The use of any DiscipleNET asset to gain unauthorized access to any off-campus computer system, e.g., unauthorized hacking.
20. The use of DiscipleNET assets for commercial purposes without written consent by the Chief Information Officer.

6.3.1.2 Email and Communications Activities

1. Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (e.g., email spam). Official communiqué’s of the University do not constitute unsolicited email.
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster’s account, with the intent to harass or to collect replies.
5. Creating or forwarding “chain letters”, “Ponzi” or other “pyramid” schemes of any type.
6. Use of unsolicited email originating from with Cornerstone University’s network of other network service providers on behalf of, or to advertise, any service hosted by Cornerstone University or connected via Cornerstone University’s network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

7.0 Monitoring

This statement serves notice to DiscipleNET clients that DiscipleNET is considered a private network of Cornerstone University and that regular monitoring of system activities does occur. Only those persons who are expressly authorized by the Chief Information Officer may engage in system monitoring.

The following are likely to be monitored on a regular basis:

- System log files which contain information pertaining to processes executed on a given DiscipleNET asset
- System directories
- Temporary and permanent storage areas

- System security logs
- DiscipleNET assets associated with reported incidents of harassment or other violations of this policy
- Any DiscipleNET asset that must be monitor to comply with local, state, and/or federal law and/or court orders
- Any activity which appears to compromise the security or integrity of DiscipleNET
- Web site access logs

8.0 Privacy

All clients, including the staff of Information Systems, should respect the privacy of other authorized clients. This includes respecting the rights of others' security of files, confidentiality of data, and ownership of their work as prescribed by other University policies.

Nonetheless, in order to enforce the policies set herein and to maintain the functionality and integrity of DiscipleNET, the Information Systems staff is permitted to monitor activity on any DiscipleNET system in accordance with guidelines established by the Chief Information Officer. In general, staff may routinely search a DiscipleNET asset for potential violations of these policies. When there is clear evidence of a violation, they may view clients' files, monitor keystrokes, and otherwise monitor clients' activities. In cases deemed especially serious by the appropriate authorities, Information Systems staff may read clients' email after obtaining permission from the appropriate authority.

If a member of the University community outside of Information Systems reports activities in apparent violation of University policy, they should notify the Chief Information Officer who will then contact other University authorities as necessary. Upon authorization, an investigation of a client's DiscipleNET activities and data may be initiated by Information Systems staff. All such investigations shall be kept on-file by the Chief Information Officer and shall be considered confidential with access only by authorized agents of the University. In the course of an investigation, evidence of violations of law will be referred to the appropriate law enforcement officials.

Cornerstone University is under no obligation to inform any client of system monitoring or access to client information in the course of an investigation.

9.0 Enforcement

Evidence of the violation of the principles described within this policy statement may result in disciplinary action. As stated previously, in cases where University policy already exists, e.g., the Discernment Policy, and the only difference was that a DiscipleNET asset was utilized to perform the activity, such action will be taken through appropriate University channels as prescribed in the governing policies. Violation of State or Federal statutes may result in civil or criminal proceedings. In other cases, those who engage in violations of this policy are subject to Information Systems or to other authorities if so referred to by Information Systems.

System administrators, with due regard for the respect of privacy of clients and the confidentiality of their data, have the authority to suspend or modify DiscipleNET access privileges, examine files, data and any other materials that may aid in maintaining the integrity and efficient operation of the system. Clients whose activity is viewed as a threat to the operation of a DiscipleNET asset, who abuses the rights of other clients, or who refuses to cease improper behavior may have disciplinary action taken against them.

Violation of the policies herein may result in one or more of the following, plus any additional actions deemed appropriate by Information Systems:

- Suspension of one's ability to perform interactive logins on relevant DiscipleNET assets
- Suspension of one's ability to send or receive email
- Increased monitoring of further DiscipleNET activity

Upon taking action, Information Systems will issue a written notification to the client within 24 hours. The notice will clearly state which policies are in violation. The notification will also detail the Information Systems staff member who enacted the suspension (the "policy agent"). The suspended client must contact the designated policy agent regarding the suspension. After discussing the violation, the policy agent may alter the suspension as appropriate or keep it in force. In the event that the client and the policy agent are unable to resolve the matter to the client's satisfaction, he or she may appeal in writing to the Chief Information Officer within five business days. The decision of the Chief Information Officer will be considered final except in cases where other University policy may supercede this policy. In the case of employees, copies of the violation and suspension will be forwarded by the policy agent to the employee's supervisor.

If a revoked privilege is needed by a student to complete academic work, the student must obtain a note signed by a professor explaining why the privilege is required and submit it to the policy agent. Only the minimum privileges needed fulfill the student's academic activities will be restored. Any further abuse by the student in question will lead to the privilege being revoked and the student will have to endure the consequences of his or actions with the respective professor.

10.0 Policy Revisions

The Chief Information Officer may change or amend this policy as needed. When changes are made, they will be announced through normal communication means.