IT POLICY – COR001-AUP

ACCEPTABLE USAGE POLICY

The Acceptable Usage Policy provides a framework for the acceptable usage of information technology (IT) resources and communication networks which aims to provide an environment and culture of openness, trust and integrity.

In addition, Cornerstone Institute is committed to protecting itself and its students, faculty and staff from unethical, illegal, or damaging actions by individuals using these systems.

TABLE OF CONTENTS

IT POLICY – COR001-AUP

ACCEPTABLE USAGE POLICY

1. PURPOSE

The purpose of the document is to outline the ethical and acceptable use of information systems at Cornerstone Institute. The policy is not intended to restrict the usage of information systems, but rather to protect students, faculty and staff. It further aims to provide a framework for reliable and robust IT resources that are safe from unauthorised or malicious use.

Insecure practices and malicious acts expose Cornerstone Institute as well as students, faculty, and staff to risks including virus attacks, compromise of network systems and services, and loss of data or confidential information. Security breaches caused by these practises damage the institute reputation and could result in loss of services. Other misuses, such as excessive us by an individual, can diminish resources available to other users.

2. SCOPE

The Acceptable Usage Policy is an integral part of IT security policies and applies to students, faculty and staff as well as any other individuals or entities who use information and IT resources at Cornerstone Institute. The policy applies to all IT resources owned and lease by Cornerstone Institute and to any privately owned equipment connected to the network and includes, but is not limited to, computer equipment, software, operating systems, storage media, the network, and the Internet.

All individuals and entities are required to know the policies and to conduct their activities within the scope of the Acceptable Usage Policy, the Information Technology Security policy, and the Policies, Standards, and Guidelines for IT Security (see additional documentation).

Failure to comply with this policy my result in loss of computing privileges and/or disciplinary action.

3. POLICY STATEMENT

Unless otherwise specified in this policy or other institutional policies, the use of the intuitional information technology resources is restricted to purposes related to the institution. Eligible individuals are provided to access in order to support their studies, instructions, duties as employees, official business with the institute, and other institution-sanctioned activities. Individuals may not share with or transfer to others their institutional accounts including network IDs, passwords, or other access codes that allow them to gain access to the institute's information technology resources.

Incidental personal use of information technology resources must adhere to all applicable institute policies. Refer to Personal Use and Misuse of Institutional Property policy (see additional documentation). Under no circumstances may incidental personal use involve violations of the law, interfere with the fulfilment of a students' studies and an employee's institute responsibilities, or adversely impact or conflict with activities supporting the mission of the institute.

4. POLICY

4.1. General Use and Ownership

4.1.1. Cornerstone Institute proprietary information stored on electronic or computing devices whether owned or leased by Cornerstone Institute, the employee, a student or a third party, remains the sole property of Cornerstone Institute. It is your responsibility to ensure that proprietary information is protected.

4.1.2. You may access, use or share proprietary information of Cornerstone Institute to the extent it is authorised and necessary to fulfil assigned job duties or further your studies as a student.

4.1.3. Students, faculty and staff are responsible for exercising good judgement regarding the reasonableness of personal use.

4.1.4. For security and network maintenance purposes, authorised individuals within Cornerstone Institute my monitor equipment, systems and network traffic at any time.

4.1.5. Cornerstone Institute reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2. Security and Proprietary Information

4.2.1. All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

4.2.2. System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4. Postings by employees from an email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the institution, unless posting is in the course of business duties.

4.2.5. Students, faculty and staff must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.2.6. Engaging in or effecting security breaches or malicious use of network communication including, but not limited to:

4.2.6.1. Obtaining configuration information about a network or system for which the user does not have administrative responsibility.

4.2.6.2. Engaging in activities intended to hide the user's identity, to purposefully increase network traffic, or other activities that purposefully endanger or create nuisance traffic for the network or systems attached to the network.

4.2.6.3. Circumventing user authentication or accessing data, accounts, or systems that the user is not expressly authorized to access.

4.2.6.4. Interfering with or denying service to another user on the campus network or using institute facilities or networks to interfere with or deny service to persons outside the institute.

4.2.6.5. Installing unauthorised programmes on a computer. Programme installations must be approved by IT.

4.3. Unauthorized Use of Intellectual Property

Users may not use institute facilities or networks to violate the ethical and legal rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations. Violations include, but are not limited to:

4.3.1. Except as provided by fair use principles, engaging in unauthorized copying, distribution, display, or publication of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources; copyrighted music or video; and the installation of any copyrighted software without an appropriate license.

4.3.2. Using, displaying, or publishing licensed trademarks, including Cornerstone Institute trademarks, without license or authorization or using them in a manner inconsistent with the terms of authorization.

4.3.3. Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws.

4.3.4. Breaching confidentiality agreements or disclosing trade secrets or pre-publication research.

4.3.5. Using computing facilities and networks to engage in academic dishonesty prohibited by institute policy (such as unauthorized sharing of academic work or plagiarism).

4.4. Inappropriate or Malicious Use of IT Systems

Inappropriate or malicious use of IT systems includes:

4.4.1. Setting up file sharing in which protected intellectual property is illegally shared.

4.4.2. Intentionally introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).

4.4.3. Inappropriate use or sharing of institute-authorized IT privileges or resources.

4.4.4. Changing another user's password, access, or authorizations.

4.4.5. Using a Cornerstone Institute computing asset to actively engage in displaying, procuring, or transmitting material that is in violation of sexual harassment policy or laws, hostile workplace laws, or other illegal activity.

4.4.6. Using a Cornerstone Institute computing asset for any private purpose or for personal gain.

4.5. Social Media

4.5.1. The use of social media by employees, whether using Cornerstone Institute's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Cornerstone Institute's systems to engage on social media is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Cornerstone Institute's policies, is not detrimental to Cornerstone Institute's best interests, and does not interfere with studies or regular work duties in any form.

4.5.2. Cornerstone Institute's Confidential Information policy also applies to social media. As such, students, faculty and staff are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by Cornerstone Institute's Confidential Information policy.

4.5.3. Students, faculty and staff shall not engage in any form of social media that may harm or tarnish the image, reputation and/or goodwill of and/or any of its students, faculty or staff. Students, faculty and staff are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when using social media or otherwise engaging in any conduct prohibited by Cornerstone Institute's Non-Discrimination and Anti-Harassment policy.

4.5.4. Students, faculty and staff may also not attribute personal statements, opinions or beliefs to when using social media. If a student, faculty member or staff member is expressing his or her beliefs and/or opinions on social media, the student, faculty member or staff member may not, expressly or implicitly, represent themselves as representative of Cornerstone Institute. Students, faculty and staff assume any and all risk associated with social media.

4.5.5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Cornerstone Institute's trademarks, logos and any other intellectual property may also not be used in connection with any form of social media activity.

4.6. Misuse of Electronic Communications

Electronic communications are essential in carrying out the activities of the institute and to individual communication among faculty, staff, students, and their correspondents. Individuals are required to know and comply with the institute's policy on **Mass Email and Effective Electronic Communication** (see Resources below).

4.6.1. Key **prohibitions** include:

4.6.2. Sending unsolicited messages, including "junk mail" or other advertising material, to individuals who did not specifically request such material, except as approved under the policy on Mass Email and Effective Electronic Communication.

4.6.3. Engaging in harassment via electronic communications whether through language, frequency, or size of messages.

4.6.4. Masquerading as someone else by using their email or internet address or electronic signature.

4.6.5. Soliciting email from any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

4.6.6. Creating or forwarding "chain letters" or solicitations for business schemes.

5. INDIVIDUAL RESPONSIBILITY

5.1. The following rules are important for the promotion of responsible usage:

5.1.1. All laptops which have wireless connectivity are required to be registered with the IT administrator and cleared of viruses before access to network is allowed.

5.1.2. Users are to report malfunctioning equipment through logging a call with IT.

5.1.3. All personal devices must have antivirus software installed on their computer in order to avoid the spread of viruses and regularly update this with the latest virus definition files.

5.1.4. Should a student, faculty member or staff member become aware of a breach or suspected breach of security, he/she is to report it to IT.

5.1.5. Complaints regarding violations should be reported to Student Services in regards to students and to IT in regards to faculty, staff and third parties.

6. ENFORCEMENT

The Acceptable Use of Information Technology Resources policy is enforced through the following mechanisms.

6.1. Interim Measures

6.1.1. The institute may temporarily disable service to an individual or a computing device, when an apparent misuse of institute computing facilities or networks has occurred, and the misuse:

6.1.1.1. Is a claim under the Digital Millennium Copyright Act (DMCA)

6.1.1.2. Is a violation of criminal law

6.1.1.3. Has the potential to cause significant damage to or interference with institute facilities or services

6.1.1.4. May cause significant damage to another person

6.1.1.5. May result in liability to the institute

6.1.2. An attempt will be made to contact the person responsible for the account or equipment prior to disabling service unless law enforcement authorities forbid it or Information Technology Services staff determine that immediate action is necessary to preserve the integrity of the institute network. In any case, the user shall be informed as soon as possible so that they may present reasons in writing why their use is not a violation or that they have authorization for the use.

6.2. Suspension of Services and Other Action

Users may be issued warnings, may be required to agree to conditions of continued service, or may have their privileges suspended or denied if:

6.2.1. After hearing the user's explanation of the alleged violation, an IT provider has made a determination that the user has engaged in a violation of this code, or

6.2.2. A student or employee disciplinary body has determined that the user has engaged in a violation of the code.

6.3. Disciplinary Action

Violations of Cornerstone Institute’s Acceptable Use of Information Technology Resources policy may be referred for disciplinary action as outlined in the Student Disciplinary Regulations and applicable faculty and staff handbooks or collective bargaining agreement. The institute may assess a charge to offset the cost of the incident.