

## Responsible Use of Electronic Communications

---

### **POLICY STATEMENT**

---

DSU does not allow use of electronic communications to:

- harass, threaten, or otherwise cause harm to a specific individual(s), whether by direct or indirect reference;
- impede, interfere with, impair, or otherwise cause harm to the activities of others;
- download or post to university computers, or transport across university networks, material that is illegal, proprietary, in violation of university contractual agreements, or otherwise is damaging to the institution; harass or threaten classes of individuals.

As a matter of policy, the university protects expression by members of its community and does not wish to become an arbiter of what may be regarded as "offensive" by some members of the community. However, in exceptional cases, the university may decide that such material directed to classes of individuals presents such a hostile environment that certain restrictive actions are warranted.

---

### **DEFINITIONS**

---

College/Unit Policy Officer: A person with responsibility for issues having broad-based policy implications for students, faculty, and staff in the college/unit; an Associate Dean or similar position.

Education Records: Records specifically related to a student and maintained by an educational institution or a party acting on its behalf. The Family Educational Rights and Privacy Act of 1974 protect these records.

Electronic Communications: The use of computers and network systems in the communicating or posting of information or material by way of electronic mail, bulletin boards, or other such electronic tools.

Network Systems: Includes voice, video and data networks, switches, routers, wireless devices, and storage devices.

System or Network Administrator: A university employee responsible for managing the operation or operating system environments of computers or network systems, respectively.

University Computers and Network Systems (University Systems): Computers, networks, servers, and other similar devices that are administered by the university and for which the university is responsible. Throughout this policy, the shortened term "university systems" is used to mean all university computers and network systems.

---

### **PROCEDURES and RESPONSIBILITIES**

---

The university seeks to enforce its policies regarding harassment and the safety of individuals; to protect the university against seriously damaging or legal consequences; to prevent the posting of proprietary software or the posting of electronic copies of literary works in disregard of copyright restrictions or contractual obligations; to safeguard the integrity of computers, networks, and data, either at Delta State or elsewhere; and to ensure that use of electronic communications complies with the provisions of the Campus Code of Conduct for maintaining public order or the educational environment.

Computers and network systems offer powerful tools for communication among members of the Delta State community and of communities outside of the university. When used appropriately, these tools can enhance dialog and communications. Unlawful or inappropriate use of these tools, however, can infringe on the rights of others. The university expects all members of its community to use electronic communications in a responsible manner.

The university recognizes the complexity of deciding what constitutes appropriate use of electronic

communications services. What is appropriate or inoffensive to some members of the community may be inappropriate or offensive to others.

Having open access to network-based services implies some risk. In a community of diverse cultures, values, and sensitivities, the university cannot protect individuals against the existence or receipt of material that may be offensive to them.

The university encourages the diversity of values and perspectives endemic in an academic institution and so is respectful of freedom of expression. The university does not condone censorship, nor does it endorse the inspection of electronic files other than on an exceptional basis (i.e., if required to ensure the integrity, security, or effective operation of university systems).

Nevertheless, the university reserves the right to place limited restrictions on the use of its computers and network systems in response to complaints presenting evidence of violations of university policies or codes, or state or federal laws. Once evidence is established, the university authorities responsible for overseeing these policies and codes will be consulted on the appropriateness of specific restrictions, which could include the removal of material posted on a computer and/or limiting access to the university's networks.

The university reserves the right to limit access to its networks when applicable university policies or codes, contractual obligations, or state or federal laws are violated, but does not monitor or generally restrict the content of material transported across those networks. The university reserves the right to remove or limit access to material posted on university-owned computers or systems, such as Exchange e-mail, when applicable university policies or codes, contractual obligations, or state or federal laws are violated, but does not monitor the content of material posted on university-owned computers. The university does not monitor or generally restrict material residing on university computers housed within a private domain or on non-university computers, whether or not such computers are attached to campus networks.

This policy is in accordance with university policies concerning harassment, use of computers and network systems generally, and related judicial codes. Any restrictive actions taken by the university will be in accordance with guidelines and procedures set forth in these policies, codes, or laws. The restrictive actions pertaining to this policy conform to the Electronic Communication Privacy Act of 1986.

In exceptional cases, a system or network administrator may detect evidence of a violation while performing his or her duties operating or maintaining a system. In such instances, the system or network administrator should contact the college/unit policy officer, his/her supervisor, or the Office of Information Technology for further guidance.

This policy does not abrogate local policies governing the operation and maintenance of university systems provided they do not conflict with the precepts of university policy. Colleges and administrative units may wish to develop ancillary procedures that support organizational requirements. Specifically, procedural guidelines with regard to security, privacy, and other areas of critical importance to the administration of these systems are not addressed as part of this policy, nor are violations of principles of network etiquette.

### **Right to Privacy**

User files on central University systems are kept as private as possible. Attempts to read another person's protected files will be treated with the utmost seriousness. The systems administrators will not override file protections unless necessary in the course of their duties, and will treat the contents of those files as private information at all times.

### **Violations**

Violations of these policies may result in the immediate suspension of computer account and network access pending investigation of circumstances and may lead to their eventual revocation. Serious violations of the policy will be referred directly to the appropriate University or outside authorities. Unauthorized use of University computing facilities can be a criminal offense. The penalties may be as severe as suspension or dismissal from the University and/or criminal prosecution.

### Electronic Mail

No electronic mail (e-mail) may be sent or forwarded through a University system for purposes that violate University statutes or regulations or for an illegal or criminal purpose. Electronic mail, like user files, is kept as private as possible. Attempts to read another person's electronic mail will be treated with the utmost seriousness. The University and its administrators of central e-mail systems will not read mail unless necessary in the course of their duties. Also, there may be inadvertent inspection in the ordinary course of managing and maintaining the computer network and in carrying out other day-to-day activities. On central systems, e-mail that cannot be delivered to one or more addressees is directed to the system administrators for purposes of assuring reliable e-mail service, in most cases as "headers-only".

Users should be aware that their "deletion" of electronic information will often not erase such information from the system's storage until it is overwritten with other data and it may, in any case, still reside in the University's network either on various back-up systems or other forms, and even if erased, may still exist in the form of print-outs. Nuisance e-mail or other online messages such as chain letters, obscene, harassing, or other unwelcome messages are prohibited. Unsolicited e-mail messages to multiple users are prohibited unless explicitly approved by the appropriate University authority. All messages must show accurately from where and from whom the message originated, except in the rare, specific cases where anonymous messages are invited.

The University reserves the right to refuse mail and other connections from outside hosts that send unsolicited, mass or commercial messages, or messages that appear to contain viruses to University or other users, and to filter, refuse or discard such messages. It should be noted that .zip file attachments are blocked, for security purposes, from entering the university network.

### Faculty and Staff Appropriate Use Statement

All faculty and staff are required to apply for a University provided e-mail account and login and password when obtaining employment with the University. All positions will require this information for use of the email and Internet capabilities of the University. Each member is required to read and sign the Faculty and Staff Appropriate Use Statement.

It is the policy of Delta State University to view information as a business asset. Misuse or damage of information may be as costly to the University as would be misuse or damage of physical property.

### Reporting Violations

If you believe that a violation of this policy has occurred, contact the system or network administrator responsible for the system or network involved, who will report the incident to the college/unit policy officer in accordance with local procedural guidelines, should they exist.

There may be situations when the following additional offices should be contacted:

- University Health Services and/or the Delta State University Police, if an individual's health or safety appears to be in jeopardy;
- University Human Resources, if violations occur in the course of employment;
- Office of Information Technology, if an incident potentially bears external or legal consequences for the institution. This office is available to assist with investigations, generally under the auspices of the college/unit policy officer. You may also contact this office if you wish to report an incident but are unable to do so through normal channels.

### Procedures for Systems and Network Administrators

When a complaint is filed and evidence is presented that a violation of this policy has occurred, proceed as follows:

1. Refer to Table 2 to determine what type of violation may apply:
  - violations targeted at a specific individual(s) (4 types identified);
  - violations causing harm to the activities of others (8 types identified);
  - violations involving illegal, proprietary or damaging material (4 types identified);
  - violations targeted at classes of individuals (1 type identified).
2. If unable to match your incident with a description in Table 2, or if multiple descriptions seem to

apply, contact your college/unit policy officer or the Office of Information Technology for guidance.

3. Follow the guidelines in Table 2. In addition to the type of violation, the guidelines are framed by other factors, specifically:
  - who reported the violation;
  - whether you administer the university system involved or some other affected system;
  - how participants or affected parties are affiliated with Delta State.
4. In all cases, these guidelines tell:
  - which university authority should receive a formal complaint;
  - the party or parties who normally file such a complaint;
  - what actions, if any, you should or may take.
5. Report the violation in accordance with these guidelines and those established by your college/unit.
  - Document the incident and any actions you take. Protect this information as you would any confidential material. Update and retain it as appropriate. This information may be subject to review by appropriate university authorities, so it is important that the information be current, complete and correct, maintained in an electronic database, and easily retrievable.

In exceptional cases, the priorities of protecting the university against seriously damaging consequences and/or safeguarding the integrity of computers, networks, and data either at the university or elsewhere, may make it imperative to take temporary restrictive action on an immediate basis. In such instances, take temporary restrictive action, preferably with the prior approval of the college/unit policy officer, pending final adjudication by the university. All restrictive actions taken must be documented and justified in accordance with this policy. If there is no designated policy officer, or if the policy officer is not immediately available, contact the Office of Information Technology for guidance or assistance.

In some instances, documentation prescribed above will constitute education records and therefore will be protected under the Family Educational Rights and Privacy Act of 1974.

**Table 1: Excerpts from Electronic Communications Codes and Policies Regarding this Policy**

| <b>Violation</b> | <b>Campus Code of Conduct for Technology Related Issues</b>  |
|------------------|--|
| A                | To refuse to comply with any lawful order of a clearly identifiable University official or employee acting in the performance of his or her duties in the enforcement of University policy   |
| B                | To forge, fraudulently alter, or willfully falsify or otherwise misuse University or non-University records (including computerized records, permits, identification cards, other documents, or property) or to possess such altered documents |
| I                | To harass, abuse or threaten another by means other than the use or threatened use of physical force   |
| K                | To steal or knowingly possess stolen property (misappropriation of data or copyrighted materials, including computer software, may constitute theft)   |
| L                | To traffic, for profits or otherwise, in goods or services, when incompatible with the interests of the University and the Delta State community   |
| Q                | To sexually harass another person via electronic or non-electronic means   |
| U                | To recklessly or maliciously interfere with or damage, in violation of University rules, computer or network resources or computer data, files, or other information   |
| <b>Principle</b> | <b>Code of Academic Integrity</b>  |
| 1                | Respect for the privacy of other users' information, even when that information is not securely protected  |
| 2                | Respect for the ownership of proprietary software  |

|                  |   |
|------------------|---|
| 3                | Respect for the finite capacity of the system and limitation of use so as not to interfere unreasonably with the activity of other users  |
| 4                | Respect for the procedures established to manage the use of the system and any and all system resources   |
| <b>Statement</b> | <b>DSU Policy Regarding Abuse of Computers and Network Systems Policy (Adopted October 2002)</b>  |
| 1                | To respect the privacy of or other restrictions placed upon data or information stored in or transmitted across computers and network systems, even when that data or information is not securely protected |
| 2                | To respect an owner's interest in proprietary software or other assets pertaining to computers or network systems, even when such software or assets are not securely protected                             |
| 3                | To respect the finite capacity of computers or network systems by limiting use of computers and network systems so as not to interfere unreasonably with the activity of other users                        |

### Violations Covered by this Policy

Table 2 (which follows) presents general information about the kinds of violations covered by this policy; the party or parties normally serving as complainant(s); the university authorities to whom complainants normally refer incidents; and the appropriate actions and/or restrictions that systems and network administrators may take upon receiving a complaint and being presented with evidence of a violation. Instructions regarding how to proceed are intended for the system or network administrator responsible for the university resource from which the incident is perpetrated or on which the offending material resides, unless specified otherwise. Following is a synopsis of the material covered by Table 2:

#### A. Violations targeted at a specific individual(s)

1. Sending repeated and unwanted (harassing) communication by electronic mail or other electronic communications
2. Sending repeated and unwanted (harassing) communication by electronic mail or other electronic communications that is sexual in nature
3. Sending repeated and unwanted (harassing) communication by electronic mail or other electronic communications that is motivated by race, ethnicity, religion, gender, or sexual orientation
4. Posting or otherwise disseminating personal or sensitive information about an individual(s)

#### B. Violations causing harm to the activities of others

1. Propagating electronic chain mail
2. Interfering with freedom of expression of others by "jamming" or "bombing" electronic mailboxes
3. Forging, fraudulently altering, or willfully falsifying electronic mail headers, electronic Directory information, or other electronic information generated as, maintained as, or otherwise identified as university records in support of electronic communications
4. Using electronic communications to forge an academic document
5. Using electronic communications to hoard, damage, or otherwise interfere with academic resources accessible electronically
6. Using electronic communications to steal another individual's works, or otherwise misrepresent one's own work
7. Using electronic communications to collude on examinations, papers or any other academic work
8. Using electronic communications to fabricate research data.

#### C. Violations involving illegal, proprietary, or damaging material

1. Electronically distributing or posting copyrighted material in violation of license restrictions or other contractual agreements
2. Launching a computer worm, computer virus or other rogue program
3. Downloading or posting illegal, proprietary or damaging material to a university computer
4. Transporting illegal, proprietary or damaging material across Delta State 's networks

#### D. Violations Targeted at Classes of Individuals

1. Posting hate speech regarding a group's race, ethnicity, religion, gender, or sexual orientation (generally does not constitute a violation of the Responsible Use policy, but may under certain circumstances)

**Table 2: General Information About Violations of this Policy**

| <b>A. Violations Targeted at a Specific Individual(s)</b>  |
|--|
| <ul style="list-style-type: none"> <li>· <b>Violation: A1</b> - Sending repeated and unwanted (harassing) communication by electronic mail or other electronic communications, <u>or</u> <b>A2</b> - Sending repeated and unwanted (harassing) communication by electronic mail or other electronic communications that is sexual in nature, <u>or</u> <b>A3</b> - Sending repeated and unwanted (harassing) communication by electronic mail or other electronic communications that is motivated by race, ethnicity, religion, gender, or sexual orientation</li> <li>· <b>Who Files Complaint:</b> Targeted individual, whether or not a member of the university community</li> <li>· <b>Who Receives Complaint:</b> Office of the Judicial Administrator</li> <li>· <b>Note:</b> Delta State's Vice-President for Academic Affairs can act upon a complaint only if the sender of the material is a member of the Delta State community. If the sender is not a member of the Delta State community, the Provost/Vice President for Academic Affairs will assist the targeted individual by referring him/her to appropriate sources of help outside the university.</li> <li>· <b>Appropriate Action if Violation is reported by Targeted Individual:</b> Provide the targeted individual with the following information: <ol style="list-style-type: none"> <li>1. "Harassment is a violation of Delta State's policies and codes, and in some cases, state or federal laws. Write the sender directly and state that you find the continued correspondence to be harassing and formally ask the sender to cease all communications with you. Save a copy of this message and any other correspondence for evidence."</li> <li>2. "If you continue to receive correspondence after formally requesting that the correspondence stop, notify Delta State's Office of the Judicial Administrator. Consultations with the Provost/Vice President for Academic Affairs Judicial Administrator are confidential."</li> <li>3. "If you are concerned about your personal safety, contact the Delta State Police or your local law enforcement agency."</li> </ol> </li> <li>· <b>Appropriate Action if Violation is Reported by Another Individual:</b> Thank the party for forwarding the information and add the following: "Harassment is a violation of Delta State's policies and codes, and in some cases state or federal laws. Complaints must be filed by the targeted person. If appropriate, please encourage the targeted person to contact Delta State's Office of the Judicial Administrator for information or assistance."</li> <li>· <b>Violation: A4</b> - Posting or otherwise disseminating personal or sensitive information about an individual(s) (Examples include postings of an individual's academic records; medical information; social security number; or similar information of a personal or confidential nature that, if disseminated, could have legal or otherwise damaging implications either for the targeted person or the institution. Personal expression by an individual about another, even if posted in a public manner, is not subject to limitation or restriction under this policy, although a targeted person may have recourse under other campus policies or codes, or state or federal laws regarding harassment.)</li> <li>· <b>Who Files Complaint:</b> Targeted individual or System or network Administrator, in accordance with guidelines established by the designated college/unit policy officer, and in response to complaint from targeted individual. (Generally, pre-preemptive</li> </ul> |

restrictive actions are not warranted but may be in exceptional cases. If the material is of such a nature that it potentially bears external consequences for the institution, contact your college/unit policy officer and the Office of Information Technology for further guidance or assistance.)

- **Who receives complaint:** Office of Information Technology
- **Appropriate Action if Violation is Reported by Targeted Individual:** Provide the targeted individual with the following information: "This material may violate Delta State's codes or policies, or possibly state or federal laws. If you wish the material temporarily restricted while you file a complaint, please contact me."

Contact your college/unit policy officer or the Office of Information Technologies for further guidance or assistance.

- **Appropriate Action if Violation is Reported by Another Individual**

Provide the party with the following information: "Thank you for forwarding this information. I will be working with campus authorities regarding this incident."

Contact your college/unit policy officer or the Office of Information Technology for further guidance or assistance.

## B. Violations Causing Harm to the Activities of Others

- **Violation: B1** - Propagating Electronic Chain Mail
- **Who Files Complaint:** System or network Administrator, in accordance with guidelines established by the designated college/unit policy officer, and in response to complaint from individual(s) receiving the chain mail.
- **Who Receives Complaint:** Office of the Judicial Administrator
- **Appropriate Action if Violation is Reported:** Provide the party with the following information and take steps outlined below:

"Although we understand that some of these letters can be offensive or unwanted, [name of unit] cannot prevent their circulation. Forwarding chain mail using university resources violates Delta State's codes and policies, and in some cases may be illegal. I will be working with campus authorities regarding this incident."

1. Post a notice to your system alerting users to the incident and instructing them not to propagate further.
2. Refer Delta State propagators to the Office of the Judicial Administrator.
3. If the propagator(s) is not a member of the Delta State community, contact the administrator of the originating system, if possible, as a matter of courtesy or follow-up.
4. Contact your college/unit policy officer and the Office of Information Technology if you believe the content of the material to be illegal, damaging, or otherwise to have external consequences for the institution.

- **Violation: B2** - Interfering with freedom of expression of others by "jamming" or "bombing" electronic mailboxes
- **Who Files Complaint:** Individuals affected by the interference; or System or network administrator, in accordance with guidelines established by the designated college/unit policy officer, and in response to complaint from individual(s) affected by the interference.
- **Who Receives Complaint:** Office of the Judicial Administrator; or Office of the College Dean (if incident is in the context of the Code of Academic Integrity; see *example incidents B4-8, below*)
- **Appropriate Action if Violation is Reported:** Provide the party with the following information and take steps outlined below:

"Attempting to interfere with the freedom of expression of others violates Delta State's Campus Code of Conduct. I will be working with campus authorities regarding this incident."

1. If the violator is a member of the Delta State community, instruct him/her to cease the activity, referring to campus policy, and contact the Judicial Administrator for further guidance.
2. If the violator is not a member of the Delta State community, contact the administrator of the originating system, if possible, as a matter of courtesy or follow-up.

- **Violation: B3** - Forging, fraudulently altering, or willfully falsifying electronic mail headers, electronic directory information, or other electronic information generated as, maintained as, or otherwise identified as university records in support of electronic communications
- **Who Files Complaint:** Individual(s) affected by the forgery or alteration, such as the recipient of fraudulent mail or the individual whose identity is forged, if applicable; or System or network administrator, in accordance with guidelines, and in response to complaint from individuals(s) affected by the forgery or alteration.
- **Who Receives Complaint:** Office of the Judicial Administrator or Office of the College Dean (if incident is in the context of the Code of Academic Integrity; *see example incidents B4-8, below*)
- **Appropriate Action if Violation is Reported:** Provide the party with the following information and take steps outlined below: "Forging, fraudulently altering or willfully falsifying university records violates Delta State's policies and codes. I will be working with campus authorities regarding this incident."

If the violator is a member of the Delta State community, instruct him/her to cease the activity, referring to campus policy, and contact the Judicial Administrator for further guidance. If the violator is not a member of the Delta State community, contact the administrator of the originating system, if possible, as a matter of courtesy or follow-up.

- **Violation: B4** - Using electronic communications to forge an academic document; or **B5** - Using electronic communications to hoard, damage, or otherwise interfere with academic resources accessible electronically; or **B6** - Using electronic communications to steal another individuals work, or otherwise misrepresent one's own work; or **B7** - Using electronic communications to collude on examinations, papers or any other academic work; or **B8** - Using electronic communications to fabricate research data
- **Who Files Complaint:** Individual whose academic work is stolen, misrepresented, or otherwise compromised or damaged; or Delta State faculty member or academic department/sponsor responsible for the academic activity
- **Who Receives Complaint:** Office of the College Dean
- **Appropriate Action if Violation is Reported:** Provide the party with the following information: "This incident may violate campus policies or codes. I will be working with college authorities to review what actions may be appropriate."
- Contact your college policy officer for further guidance.

### C. Violations Involving Illegal, Proprietary, or Damaging Material

- **Violation: C1** - Electronically distributing or posting copyrighted material in violation of license restrictions or other contractual agreements; or **C2** - Launching a computer worm, virus, or other rogue program; or **C3** - Downloading illegal, proprietary, or damaging material to a university computer; or **C4** - Transporting illegal, proprietary, or damaging material across Delta State's networks
- **Who Files Complaint:** Anyone who has evidence of such activities occurring or about to occur, and involving Delta State's computer and network systems

- **Who Receives Complaint:** Office of Information Technology
- **Appropriate Action if Violation is Reported:** Commensurate with the degree of urgency and potential damage to the institution, take pre- preemptive steps - preferably with the approval of your college/unit policy officer - including ensuring the preservation of evidence. Contact the Office of Information Technology for further guidance or assistance.
- Clarification regarding **C1:** Responsible Use policy and procedures govern incidents involving the illegal *distribution* of copyrighted material - as transported through Delta State's networks or posted to Delta State's computers - by electronic means. The *possession* of misappropriated copyrighted material by a member of the Delta State community violates the Campus Code of Conduct, the Code of Academic Integrity and the university's policy on the Abuse of Computers and Network Systems.

#### D. Violations Targeted at Classes of Individuals

- **Violation: D1** - Posting hate speech regarding a group's race, ethnicity, religion, gender, or sexual orientation Note: Posting hate speech generally does not constitute a violation of Responsible Use Policy, but may under certain circumstances.
- **Who Files Complaint:** Member of the targeted group; or system or network administrator, in accordance with guidelines established by the designated college/unit policy officer, and in response to complaint from member(s) of the targeted group.
- **Who Receives Complaint:** Office of Human Resources
- **Appropriate Action if Violation is Reported:** Provide the party with the following information:  
'Although this posting/communication may be offensive to members of the community, the university is respectful of expression in its own right. However, this posting/communication may constitute harassment, which is a violation of Delta State's policies and codes, and in some cases, state or federal laws. I will consult with campus authorities regarding this incident.'

---

#### RELATED DOCUMENTS

---

- Faculty and Staff Appropriate Use Statement
- Student e-mail policy

Copyright © 2008 Delta State University. All rights reserved.  
Delta State University, Highway 8, Cleveland, MS 38733 1-800-GO-TO-DSU