NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

SEC. VII — E-MAIL 3.0

STUDENT EMAIL USE

University Policy

I. Scope

The purpose of this policy is to ensure the proper use of North Carolina Agricultural and Technical State University's email accounts for undergraduate and graduate students using the University's domain name email (aggies.ncat.edu) pursuant to an agreement between the University and Google, Inc. (the "Gmail Accounts"). Electronic Mail is a tool provided by the University to complement traditional methods of communication and to improve education and administrative efficiency. Users have the responsibility to use this resource in an efficient, effective, ethical and lawful manner. Violations of policy may result in restriction of access to the Gmail Accounts and/or other appropriate disciplinary action. In the event a University student holds both a University Email Account and a Gmail Account, the rules of the policy specified for the University Email or Gmail use shall apply based on the email account being used (University Email Policy for University Email usage, Gmail Policy for Gmail usage).

II. Policy Statement

A. Account Creation

University Gmail Accounts are created based on the legal name of the student as initiated by the Undergraduate Admissions and Graduate Admissions offices. The format of user names will be based on the user's first initial, middle initial (if applicable), and last name. If the generated user name has already been used, a sequential number will be appended to the user name. Requests for email aliases based on name preference, middle name, nicknames, etc., cannot be accommodated. An existing email username already in use before the change to the standardized format will be kept as an email alias to the new username. Only requests for name changes to correct a discrepancy between an email account name and official University records will be processed, in this case the email account name will be corrected. User id's will remain in the University's system and will not be reused at any time.

B. Ownership of Email Data

The University owns the Gmail Accounts and the messages in those accounts. Subject to underlying copyright and other intellectual property rights under applicable laws and University policies, the University also owns data received, transmitted, or stored using the Gmail Account.

C. Privacy and Right of University Access

Messages on an assigned Gmail Account are the property of the University, are a public record, and may be viewed at the discretion of the University. Users of Gmail Accounts should not have any expectation of privacy or confidentiality for personal messages in their account.

Under certain circumstances, it may be necessary for the DoIT staff or other appropriate University officials to access Gmail Accounts; these circumstances may include, but are not limited to, maintaining the system, investigating security or abuse incidents, investigating alleged violations of this or other University policies, violations of Google's Acceptable Use Policy, or the University's contract with Google.

Google also retains the right to access the Gmail Accounts for violations of its Acceptable Use Policy.

Should the student relationship between the University and student terminate, access to personal email located on a Gmail account will be terminated as well. North Carolina Agricultural and Technical State University assumes no responsibility to provide access or support of personal email transmitted or received to a Gmail account.

D. Data Purging

Google currently provides the following guidelines for purging folders:

Trash – 30 days
Spam – 30 days

E. Data Backup

There is no restoration services ensured for the Gmail Accounts. A reasonable effort will be made to assist in recovering accidently deleted email from a Gmail account.

F. Expiration of Accounts

Individuals who separate from the University will have their Gmail accounts purged. There are many situations at the University where the expiration of accounts will differ, as set forth below. The University reserves the right to remove email privileges at any time subject to the following guidelines:

A Gmail account will be established for a student upon admission to the University. At the census date of the semester, the Gmail account of prospective students not enrolled in the University are purged. If a student has indicated that he/she will elect a deferred enrollment, the Gmail account will be retained until the census date of the following year. If a deferred student has not enrolled by the census date following one (1) year of the intent to defer, the account will be purged.

One (1) year after a current student is shown as not enrolled, the Gmail account will be purged

A student who is expelled – If a student is expelled from the University, email privileges will be terminated immediately upon the directive from the Dean of Student's Office.

G. Appropriate Use

When using email as an official means of communication students must apply professionalism, discretion, respect and standards appropriate for university communication. All email is subject to public records/disclosure laws. Users of email shall not disclose information about students and/or employees in violation of University policies or laws protecting the confidentiality of such information.

The Data Classification Policy (http://www.ncat.edu/legal/policies/sec7-info-tech/data%20classification.pdf) is applicable to all users that have University issued e-mail accounts. Emailing restricted data is subject to protective governance including but not limited to federal and state statutes/regulations, industry standards, and University policies. University divisions, offices, and organizations that collect employee, student, alumni, vendor, and guest data are responsible for understanding and abiding by email regulations,

standards, and policies that pertain to restricted personnel, medical, financial, University business, and research data.

Approval and transmission of email containing essential University announcements to students, faculty, or staff must be obtained from the responsible University official noted as follows:

- for sending to all faculty, approval from the Provost and Vice Chancellor for Academic Affairs,
- for sending to all staff, approval from the Vice Chancellor for Human Resources,
- for sending to all students, approval from the Vice Chancellor for Student Affairs.
- for sending of information technology communications, Vice Chancellor for Division of Information Technology.

Use of distribution lists or 'reply all' features of email should be carefully considered and only used for legitimate purposes as per these guidelines. In some cases where email messages generate a high number of responses due to the subject matter, it may be appropriate to utilize the University's survey software available through the Department of Institutional Research.

H. User Responsibility

A & T DoIT maintains the University's official email system. Students are expected to read email on a regular basis and manage their accounts appropriately. An email message regarding University matters sent from an administrative office, faculty, or staff member is considered to be an official notice.

Sharing of passwords is strictly prohibited. Each individual is responsible for his/her account, including the safeguarding of access to the account. All email originating from an account is deemed to be authored by the account holder (unless proven to the contrary), and it is the responsibility of that holder to ensure compliance with these policies. Users must change their passwords every 90 days. Detailed information can be found at: http://www.ncat.edu/divisions/doit/dept/ats/change-password.html

I. Supported Mail Clients

The University-supported web portal for Gmail is located at: https://mail.aggies.ncat.edu for students. The Division of Information Technology will not support alternate email clients. Helpdesk personnel will work with the individual to access email via the supported method and will verify functionality of the supported environment. The University Division of Information Technology is continually evaluating tools and technologies and reserves the right to modify the list of supported clients with appropriate notification.

J. Inappropriate Use

All Gmail Accounts are subject to Google's Acceptable Use Policy (http://www.google.com/a/help/intl/en/admins/use_policy.html). Any inappropriate email usage, examples of which are described below and elsewhere in this policy, is prohibited. Users receiving such email should immediately contact DoIT.

- Generation of email related to any political activities.
- Generation of email for personal financial gain.
- Generation or facilitation of unsolicited bulk commercial email.
- Infringement upon another person's copyright, trade or service mark, patent, or other property right or intending to assist others in defeating those protections.
- Violation of or encouragement of violation of, federal and/or state laws and/or the legal rights of others.
- Is for any unlawful, invasive, defamatory, or fraudulent purpose.
- Intentionally distributing viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature.
- Interfering with the use of the email services, or the equipment used to provide the email services, by customers, authorized resellers, or other authorized users.
- Altering, disabling, interfering with or circumventing any aspect of the email services.
- Testing or reverse-engineering the email services in order to find limitations, vulnerabilities or evade filtering capabilities.
- Constituting, fostering, or promoting pornography.
- Inciting violence or threatening violence against one or more persons or property, or containing unlawfully harassing content.
- Creating a risk to a person's safety or health, creating a risk to public safety or health, compromising national security, or interfering with an investigation by law enforcement.
- Improperly exposing trade secrets or other confidential or proprietary information of another person.
- Misrepresenting the identity of the sender of an email.
- Using or attempting to use the accounts of others without their express permission.
- Collecting or using email addresses, screen name information or other identifiers without the consent of the person identified (including, without limitation, phishing, Internet scamming, password robbery, spidering, and harvesting).
- Using the service to distribute software that covertly gathers information about a user or covertly transmits information about the user.
- Any conduct that is likely to result in retaliation against the University's network or website, or the University's employees, officers or other agents, including engaging in behavior that results in any server being the target of a denial of service attack (DoS).

These guidelines provide some examples of permitted or prohibited use of email. This list is not intended to be exhaustive but rather to provide some illustrative examples.

K. SPAM & Virus

Incoming email is scanned for viruses and for messages deemed to be 'SPAM', or unsolicited advertisements for products or services sent to a large distribution. Suspected messages are blocked from the user's inbox. Due to the complex nature of email, it is impossible to guarantee protection against all SPAM and virus infected messages. It is therefore incumbent on each individual to use proper care and consideration to prevent the spread of viruses. In many cases viruses appear to be sent from a friend or other student, therefore attachments should only be opened when the user is sure of the nature of the message. If any doubt exists, students should contact the Aggie Tech Support Helpdesk at: (336) 334-7195 and forward a copy of the email to spam@ncat.edu

III. Enforcement

Enforcement of this policy includes the following:

- Divisional and departmental assessments
- External and internal audit compliance

University sanctions for a student cited for policy violations include but are not limited to one or more of the following:

- Suspension of information system(s) privileges. [In order to reduce the number of credentials used to access University resources, single sign-on/reduced sign-on identity management solutions are enabling users to access multiple resources with the same credentials. Suspended access will impact a student's ability to complete academic requirements and/or an employee's ability to perform his or her job duties.]
- Misconduct review.
- Discharge of employment.
- Student dismissal.
- Breach of contract/agreement filed against guests.

For University employees and students, sanctions will be administered in accordance with the Student Handbook, the Faculty Handbook, University Policies, and the Office of State Human Resources policies.

Date Policy is Effective: Upon approval

Approved by the Board of Trustees

First approved: November 22, 2013
Revised: