

## Andrew College

### Acceptable Use Policy for Informational/Communications Systems

Andrew College makes available computer, telephone, and other communications resources to support the academic research, instructional, administrative, and student services activities of the institution. The resources are intended for the sole use of Andrew College faculty, staff, students and other authorized users. These resources include, but are not necessarily limited to, host computer systems, personal computers and workstations, telephone/communications networks, software, and computer files. These policies apply to all Andrew College faculty, students, staff, and other authorized users.

- Use of Andrew College informational/communications system resources must be consistent with the College's conduct policies published in the *Faculty Handbook*, the *Personnel Handbook*, and the *Student Handbook*, as well as state and federal laws.
- Connection of personally owned computers/devices to an Andrew College system makes them subject to established usage policies.
- In order to protect the integrity of its informational/communications systems Andrew College reserves the right to gain access to all information utilizing the system(s). Access to non-public information (ie e-mail and voice mail) is limited to designated administrators and only within established guidelines.
- Access/Addresses/Accounts/Passwords granted to individuals are intended for the sole use of that individual, and are non-transferable.
- The owner is responsible for all usage on their assigned Access/Address/Account/Password.
- Andrew College expressly disclaims any liability or responsibility arising from access to or use of information obtained through electronic information systems; and encompassing any activities by a user found to be illegal, or any consequences thereof.
- The right to use the Andrew College informational/communications systems can be revoked if misused or abused, even if unintentionally.
- The following types of activities are examples of behavior that are unethical and unacceptable, and in some case may violate state or federal law:
  1. Violating copyright and/or software agreements;
  2. Altering system software or hardware configurations;
  3. Accessing another individuals' account, private files, voicemail, or e-mail without permission of the owner;
  4. Misrepresenting one's identity in electronic communication;
  5. Violating rules or codes of conduct set by services (such as Galileo and Endeavor) subscribed to by the College;
  6. Using College computing/communications systems to threaten or harass;
  7. Using College computing/communications systems for commercial or profit making purposes without written authorization from the College administration;
  8. Failure to follow established policies, procedures, and protocol.

9. Accessing websites/information/material through the misrepresentation of age or other requested information.

- Policies and regulations of the College, and state and federal law, are applicable to all resources. Alleged violations of laws, policies, procedures, or protocol will be processed as outlined under *Misuse of Andrew College Informational Communications Resources*.

**I have read and understand the above Acceptable Usage Policy and hereby agree to abide by all established policies and procedures.**

\_\_\_\_\_ (Printed Name)

(Signature) / / (Date)

## Andrew College

### Misuse of Andrew College Informational/Communications Resources

Individuals who misuse Andrew College informational/communications systems by failure to comply with the Acceptable Use Policy, are subject to loss of access to those resources as well as other disciplinary action, depending upon the nature of the breach of policy. In instances in which the alleged violations involve state/federal laws or institutional conduct policies such as sexual harassment or non-discrimination, the disciplinary procedure outlined in the *Faculty or Personnel or Student Handbook* will have precedence. Actions regarding access to informational/communications resources will be based upon the determination of that process.

1. Individuals who have allegedly violated established policies/procedures will be notified in writing of the alleged violation by the Vice President for Finance. A copy of the notification will be given to the Dean of Student Affairs if the individual is a student; the Dean of Academic Affairs if the individual is a faculty member; or to his/her supervisor if the individual is a staff member.
2. A hearing will be held by the Technology Committee to hear evidence in support of the alleged violation. The individual accused of the violation will be given opportunity to dispute and/or explain the alleged violation.
3. Following the hearing the Technology Committee will determine whether or not a violation took place and, if so, establish restrictions and/or the loss of access to informational/communications resources. The determination of the Committee will be given to the individual in writing.
4. The individual has the right to appeal if they feel that their hearing by the Committee was not fair and impartial. The appeal should be in writing and made to the President of the College within 24 hours. The President will appoint an appeals committee of three faculty and one staff member to review the hearing process and procedure. The appeals committee will make a recommendation to the President whose decision is final.

## Andrew College

### Administrative Access to Informational/Communication Systems Data

In order to protect the integrity of its informational/communications systems Andrew College reserves the right to gain access to all information residing in the system(s). Data, information, and/or files which directly relate to system operation/performance (*System Information-Public*) may be accessed by systems personnel on a routine basis as a defined part of their job description. Access to data, information, and/or files related to the administration or operations of the institution (*Institutional Information-Public*) are limited to specific needs and departments as defined by Federal Right-To-Privacy regulations and job description. Data, information, and/or files which do not fall in either of the above two categories (*System Information-Public* or *Institutional Information-Public*) are considered to be restricted and is classified as *Non-Public Information*. Voice-mail, e-mail, and non-system files stored on the hard drive of a workstation are examples of *Non-Public Information*. Access to *Non-Public Information* is limited to designated personnel and only within the guidelines outlined below.

Access to *Institutional Information-Public* or *Non-Public Information* without proper authorization is a serious violation of College policy and subject personnel to disciplinary action including possible dismissal.

Procedure for access to *Institutional Information-Public* or *Non-Public Information*:

1. Authorization for access to data contained in files classified as *Institutional Information-Public* or *Non-Public Information* must be granted before the fact.
2. Need for access to *Institutional Information-Public* or *Non-Public Information* must be communicated in writing by systems personnel to the Vice President for Finance. The request must be specific in regards to the information/files to be accessed, the expected time frame (beginning and ending) that access will be required, and the reason access is necessary. The Vice President for Finance may approve access to *Institutional Information-Public* based upon Federal Right-To-Privacy regulations and job description.
3. For access to *Non-Public Information* the Vice President for Finance may (1) obtain the written authorization of the author/recipient of the information, or (2) obtain written authorization from both the Dean of Academic Affairs and President of the College. Access to *Non-Public Information* without the written authorization of the author/recipient will be granted only under court-order; when there is evidence that the Andrew College informational/communications systems are being used for illegal purposes; or when the safety and/or well-being of individuals or the College community are involved.
4. Upon termination of the employer-employee relationship all *Non-Public Information* is reclassified as *Institutional Information-Public*. The Vice President for Finance may authorize the purging of all such information from the system(s). It is the responsibility of the employee to remove all his/her *Non-Public Information* from the Andrew College system(s) prior to termination of the employment relationship.

**Andrew College**  
**Administrative Access to Informational/Communication Systems Data**  
**Request and Authorization Form**

**Access to *Institutional Information-Public* or *Non-Public Information* without proper authorization is a serious violation of College policy and subject personnel to disciplinary action including possible dismissal.**

Classification:	<i>Institutional Information-Public</i>	<i>Non-Public Information</i>
Author/Recipient (if <i>Non-Public Information</i> ):	_____	
Access Requested By:	_____	
Location of File(s):	_____	
Reason Access Is Required:	_____ _____	
Time Frame: Beginning Date:	___/___/___	Ending Date: ___/___/___
Author/Recipient Authorization:	_____	Date: ___/___/___
Vice President for Finance Authorization:	_____	Date: ___/___/___
Dean of Academic Affairs Authorization:	_____	Date: ___/___/___
President Authorization:	_____	Date: ___/___/___