Guidelines Regarding Access to the 
Administrative Computing System

The following procedures to obtain access to the administrative computing system are in compliance with federal laws (Family Educational Rights and Privacy Act of 1974 as amended) and Allegheny College policy (Policy on the Privacy of Student Records, 1997).

What is the Administrative Computing System?
The Administrative Computing System is actually a collection of several systems located around the campus. These systems include, but are not limited to, the following: the main information system (Colleague), the Development Office system (Benefactor), the historical archives (Data Warehouse), the library tracking system, and the Physical Plant workorder system. For more information on systems included in this definition, contact Administrative Computing Services.

What is Inquiry access?
Inquiry access is a tool by which certain information stored on computer files at Administrative Computing Services may be viewed on a computer workstation but not changed. On-line access allows an authorized user the opportunity to view information about specific individuals. In addition, some data may be updated by authorized individuals who are given “Update” access.

What is Query access?
Query access provides an avenue by which institutional data stored in current and historical files at Administrative Computing Services may be retrieved. Query access allows an authorized user the opportunity to select populations and retrieve summary information for evaluative and planning purposes and detailed reports for operational purposes.

Who may request access?
All data contained in the Allegheny College Administrative Computing System is the property of the College, and security of confidential computer data is a matter of major College concern. Administrative Computing Services, in conjunction with other offices, maintains records of and controls the process of access to such data. Approval for access will be evaluated by examining the person’s need to know based upon “legitimate educational interest” as outlined in the Policy on the Privacy of Student Records.

What is the access request and approval process for regular and temporary employees and consultants?
Access to general student information (as defined by the Datatel Ongoing Implementation Team) is available to employees with approval from their supervisor. This type of access usually is limited to inquiry access only. Each person with access to the Administrative Computing System must read and sign an Agreement Regarding Access form which acknowledges the person’s responsibilities for system security and confidentiality of information.

For access to additional data, the College requires that a Request for Additional Access form be submitted to Administrative Computing Services for each individual who is to have access. Each request for access is individually evaluated by Administrative Computing Services in conjunction with the offices that are responsible for the maintenance of the data to which access is being sought. It is expected that only those persons identified on request forms will have access to the system; therefore, access must be requested for each person in order to maintain system security.
Access is issued to a person, not a position or a workstation. This approval should be reviewed each year by the appropriate supervisor in conjunction with Administrative Computing Services.

The Agreement Regarding Access form and the Request for Additional Access form (if applicable) will be kept on file by the Human Resources Department and by Administrative Computing Services. Additionally, potential users may be asked to participate in appropriate training before access is granted.

**What is the access request procedure and approval process for student employees?**

Before students can have access to the Administrative Computing System, the College requires that a Student Employee Account be created for the requesting office by Administrative Computing Services. The type of access available via the Student Employee Account will be determined by the supervisor of the requesting office, Administrative Computing Services, and the offices that are responsible for the maintenance of the data to which access is being sought. This approval should be reviewed each year by the office supervisor in conjunction with Administrative Computing Services.

Before a student employee can be given access to the account, s/he must read and sign the Agreement Regarding Access acknowledging an understanding of the person’s responsibilities for password security and maintaining the confidentiality of the data that s/he accesses. This signed agreement is kept on file by the supervisor. Additionally, student users must participate in appropriate training before access will be granted.

**What are the responsibilities of persons with access?**

Each person approved for access is responsible for security of his/her password and protection of information. The authority to access is linked to a person’s user ID and password on the system. At no time should any individual share his/her password with another person or display the password in public view. Each person approved for access is responsible for logging off the system when finished with access.

It is the expressed understanding of the College that information available to an individual via access to the Administrative Computing System will be used only for the purposes for which it was intended and will not be released to others without approval. Users having access to individual records should be aware that there are possible criminal and civil sanctions and College disciplinary actions (up to and including termination) for violating records privacy agreements.

Users are responsible for knowledge of and compliance with the Allegheny College Policy on the Privacy of Student Records as information gained via access to the computer system is used.

Confidential information about individuals must be handled in a secure fashion, such that it cannot be viewed by unauthorized individuals by screen access, file access, or in printed form. Although it is allowable to print a report or screen of confidential information for authorized record keeping or advising purposes, the user should not release the printed information to others without permission. Any personally identifiable confidential data contained in print form which is no longer needed should be destroyed in such a way that individual identification is not possible.
What happens when a user terminates employment?
As a personnel change occurs, the supervisor must notify Administrative Computing Services in order to initiate access deletion when a user terminates employment or transfers to another department. A new request for access must be submitted for the person’s replacement.

What happens if a security violation is detected?
The user should immediately change his/her password (or have Administrative Computing Services reset it) and notify his/her supervisor. The supervisor is responsible for contacting Administrative Computing Services when a password security violation has been detected.

Who does a user contact with questions about access?
Questions regarding equipment, hook-up, or access should be directed to Administrative Computing Services. Questions about data found in student records should be directed to the office responsible for the maintenance of that information.