

Data Stewardship and Access Policy

POLICY:

All College information will be used with appropriate and relevant levels of access and with sufficient assurance of its integrity in compliance with existing College policies, laws, rules, and regulations.

Rationale:

Reasonable procedures need to be provided for the College community to follow to ensure that valuable College data can be utilized appropriately with guidelines for management and access to data. Roles and responsibilities need to be defined and applied to those in stewardship positions regardless of the actual purpose of the information system.

Standards & Procedures:

Standards:

This policy applies to College Information only (as defined below) and is intended to improve access to these data by employees for conducting College business. In all cases, applicable statutes, rules, and regulations that guarantee either protection or accessibility of institutional records will take precedence over this policy. While this policy is especially pertinent to information stored electronically, it is applicable to all information, such as paper, microfilm, and video, as well as the content of confidential meetings and conversations. This policy does not apply to notes and records that are the personal property of individuals in the College community and is not directed to data whose primary purpose is scholarly (e.g., instructional material, research notes)

College Information. A data element is considered College Information if it provides support to and meets the needs of units of the College.

Guidelines for determining College Information. Must meet one or more of the following:

- a) It is used for planning, providing, managing, reporting, or auditing a major administrative function
- b) It is included in an official College administrative report
- c) It is used to derive an element that meets the criteria above

By default, all College Information will be designated as INTERNAL DATA for use within the College or to satisfy College external reporting requirements to the Board of Regents of the University System of Georgia, State, Federal, or other external agencies. College employees will have access to these data for use in the conduct of College business. These data, while available within the College, are not designated as open to the general public unless otherwise required by law.

Data Categories. Data stewards are responsible for categorizing all College Information data elements within their managed systems into one of three categories: Confidential, Sensitive, or Unrestricted.

Confidential data. Requires the highest levels of restriction due to risk of harm that may result from disclosure or inappropriate use. This includes information whose improper use or disclosure could adversely affect the ability of the College to accomplish its mission, records about individuals requesting protection under the Family Educational Rights and Privacy Act of 1974 (FERPA), or data not releasable under the Georgia Open Records Act or the Georgia Open Meetings Act.

Sensitive Data. Users must obtain specific authorization to access these elements since unauthorized disclosure, alteration, or destruction will cause perceivable damage to the College. It is assumed that all administrative output from the central administrative systems is classified as sensitive unless otherwise indicated. The specification of data as sensitive should include reference to the legal or externally imposed constraint that requires this restriction, the categories of users typically given access to the data, and under what conditions or limitations access is typically given.

Unrestricted Data. No access restrictions. Available to the general public.

Data Access and Stewardship Procedures. Data users are expected to access College Information only in their conduct of College business, to respect the confidentiality and privacy of individuals whose records they access, to observe any ethical restrictions that apply to data to which they have access, and to abide by applicable laws, rules, regulations, or policies. Data stewards will work together to define a single set of procedures for requesting access to sensitive elements of College Information and to document these data access request procedures. Data stewards also have the responsibility for documenting the meta-data about their data so that users are aware of the definitions, restrictions, or interpretations, and other issues which ensure the correct use of the data.

Functional Data Classifications. Data stewards represent functional areas of the College as defined by the primary purpose served by the data. A functional unit may be given authority for data that is shared by many organizational units of the College.

Auxiliary Data. Supports the auxiliary and related enterprises of the College such as retail sales, central supplies, and other services.

Development/Alumni Data. Supports all aspects of alumni and development data. This includes personal data, demographic data, income, and giving data.

External Relations Data. Supports activities, which interface between the College and the rest of the community. This includes Event Ticket Sales, publications and public information.

Facilities Data. Supports the facilities and services resource of the College including space planning data, construction, maintenance and operational data, reservations and physical descriptive data.

Financial Data. Supports the management of fiscal resources of the College and includes accounting, budgeting, purchasing, accounts payable, accounts receivable, loans, investments, capital assets, inventory, and payroll information.

Human Resources Data. Supports the management of employee resources of the College. This data includes employee demographics, benefits, retirement and EEO data, vitas, employee evaluations, promotion and disciplinary data.

Information Technology Data. Supports the provisioning and management of the technology infrastructure provided by Information Systems and Technology. This includes email addresses, registry and directory data elements not belonging to another data type, network data, and systems data.

Library and Information Resource Data. Supports the management activities and information resource collection activities of the College libraries, including databases of purchased and locally produced information and digitized files of College archives and other special collections.

Person Registry Data. Supports the management of identity and authentication for individuals associated with the College, including the creation of unique data elements (such as DCid, MyDC user name, Library Barcode) that provide unambiguous identification and resolution for merging of identity records. Person Registry data can be used to provision other applications that are managing privileges to authorized individuals or groups.

Student Data. Supports all phases of a student's relationship with the College from application through alumni status except as noted elsewhere. This includes, but is not restricted to, demographic data, academic record, disciplinary and medical records, course information, admissions data, and financial aid, as well as employment with the College, which is dependent on student status.

Procedures:

Request for Access to College Data

Office of the Registrar
Darton College
Request for Access to Restricted Data

1. REQUEST FOR ACCESS [to be completed by Requesting Supervisor]

A. Need for Access

1. Identify the employee for whom access to the Student Records and Schedule of Classes files is being requested.

(Full) Name: _____

Employee ID/SSN: _____ (Former Name) _____

Title: _____

Department: _____

User ID: _____

2. Is this person replacing an employee who had access?

If yes, who _____ and did this person leave this position for another at Darton? (Y N)

Should access to the Student Records system be deleted for this person? (Y N) If yes, Immediately Future date _____

3. The general duties of this person include (check all that pertain):

Advise students on their academic progress/requirements

Evaluate applications for admission

Maintain student records/monitor academic progress

Coordinate course offerings and class scheduling

Look up student information

Only public (directory) information

Public and restricted information

Coordinate student class roster and grade collection

Develop and submit programs to retrieve student or course information. If so, what student and course populations will be reported?

Has employee had BANNER training? Yes No

B Access to Data

Check the boxes of the data categories below that pertain to the kind of access this person needs. Note how the information will be used, for example, advise students, monitor academic progress, etc. The use of information must relate to the responsibilities of the person as noted on page 1. Also, note in the Use of Information column any specific online screens to which the requestor needs access. Unless noted, access will be evaluated based upon general responsibility profiles.

Category of Data	Access Type		Use of information and Specific Access if applicable
	On-line Screen Retrieval		
	View	Update	
Student Academic	<input type="checkbox"/>	<input type="checkbox"/>	
Student Address Information	<input type="checkbox"/>	<input type="checkbox"/>	
Student Administrative Data	<input type="checkbox"/>	<input type="checkbox"/>	
Student Course Data	<input type="checkbox"/>	<input type="checkbox"/>	
Student Registration Data	<input type="checkbox"/>	<input type="checkbox"/>	
Student Statistical Data	<input type="checkbox"/>	<input type="checkbox"/>	
Admission Information	<input type="checkbox"/>	<input type="checkbox"/>	
Financial Aid	<input type="checkbox"/>	<input type="checkbox"/>	
Recruiting	<input type="checkbox"/>	<input type="checkbox"/>	
Historical	<input type="checkbox"/>	<input type="checkbox"/>	
Class Roster Data	<input type="checkbox"/>	<input type="checkbox"/>	
Schedule of Classes Data	<input type="checkbox"/>	<input type="checkbox"/>	
Degree Audit	<input type="checkbox"/>	<input type="checkbox"/>	
Degree Information	<input type="checkbox"/>	<input type="checkbox"/>	
Other: _____	<input type="checkbox"/>	<input type="checkbox"/>	
_____	<input type="checkbox"/>	<input type="checkbox"/>	

II. Authorization of Access

ف It is expected that your online access will be added to the Darton College security accounts tables as of _____. Your authorization to access will be included with your BANNER password.

فYour on-line access profile will be released to your Supervisor. It is the responsibility of your Supervisor to orient you to the transactions to which you have been given access. Training for direct access to files will be provided by Darton Office of Information Technology (OIT).

فYour on-line access profile will be released to your Supervisor after an orientation session with the Office of the Registrar contact person. This orientation program will include both general information and specific items tailored to your particular unit's needs, including a description of the current batch and on-line Student Record and Schedule of Classes Systems, the processing schedules for certain types of data, viewing on-line transactions and security.

ف Authorization to the information center files will be issued to you by Darton OIT. Training for access to the files will be provided by Darton OIT.

Signature of Darton College Registrar

Date of approval

ACCEPTANCE OF RESPONSIBILITY

(This form must not be completed unless the request for access has been approved by the registrar)

I understand my acceptance of access to the Student Records and Schedule of classes system signifies I accept the responsibility for complying with the institutional policy for the Release of Student Information. I have been given copies of and have read the Release of Student Information policy and the Explanation of Access guidelines. By my signature below, I understand and agree to preserve the security and confidentiality of information I access.

I will also inform my Supervisor (who will inform the office of the Registrar) when my need to access student and course data differs from the stated in this Access Request document.

I understand I am responsible for the personal security of my password.

Signature of Darton Employee

Date

I am responsible for providing an orientation program for the employee or making arrangements for staff from the office of the Registrar to provide the orientation. I will inform the Office of the Registrar contact person of any changes in status of this employee. I will initiate access deletion if this employee leaves the current position for which he/she has been given approval, and will initiate a new Access Request document for this employee's replacement, if appropriate.

Signature of Supervisor

Date