

Banner Account Request Form

Account Name: _____ (please print first, middle, last)

Banner ID: _____

UNCA Email: _____

Department: _____

Phone: _____

I have read and I understand my legal responsibilities regarding data usage which are on page 2 of this form.

Signature: _____ Date: _____

Banner Navigation Training is required and can be scheduled by calling Adrienne Oliver at 232-5005 (aoliver@unca.edu).

Department Head Authorization:

Your signature indicates that the Banner Account being created is for the above listed person and is appropriate for their job duties. **Please contact the appropriate area data security manager, shown below, to request access to university data.** This access is contingent on the approval of the Data Manager who can provide guidance on what security to apply for the requested account.

Actual access to data is granted by the data managers who have responsibility for university data. There will be no data accessible until one of the data managers notifies ITS Security to grant the access you are requesting. **You are responsible for notifying ITS if the account is no longer needed because of job duty changes.**

An annual recertification of this request will be conducted by ITS Administrative Information Systems and kept on file for audit purposes.

This account is for an employee ___ volunteer ___ student ___ other _____
(specify)

Department Head Signature	Date	Supervisor Signature	Date
---------------------------	------	----------------------	------

Data Security Managers:

Financial	Lydia Gossett	-	lgossett@unca.edu
Student Records*	Debbie Race	-	drace@unca.edu
Admissions	Patrice Mitchell	-	pmitchel@unca.edu
Financial Aid	Beth Bartlett	-	bbartlett@unca.edu
Human Resources*	Lisa Honeycutt	-	lkhoneyc@unca.edu
Alumni & Devop.*	Julia Fuog Caudill	-	jcaudill@unca.edu
NCCCR	Mike Honeycutt	-	mahoneyc@unca.edu
Accounts Receivable	Phillip Turbyfill	-	pturbyfi@unca.edu

*May grant access to general person information (name, address, biographical, etc.)

UNC Asheville is committed to protecting its information resources from accidental or intentional intrusion or damage and is equally committed to preserving and nurturing the open, information-sharing requirements of its academic culture.

The privacy of student and employee information is protected by federal laws, FERPA, HIPPA and state laws referring to the use of social security and credit card numbers. Moreover, UNC Asheville imposes its own policies regarding the safeguarding of the universities assets. Please review the policies governing use of UNC Asheville's computing resources and networks at www.unca.edu/compcenter/policies

Student Data:

Non **Directory** information as defined by FERPA may not be released to a third party without written consent of the student. Third party includes anyone who does not have a "legitimate educational interest" in the student record. Information may be shared with other University employees in the completion of work only. Non Directory information may not be shared with the student's parents without written permission.

Directory Information

- Student's Name
- Address (local, home, permanent)
- Telephone numbers
- Place of Birth
- Field of Study (major)
- Class Level (freshman, sophomore, etc.)
- Record of participation in official sports and activities, including height and weight of athletic teams
- Dates of attendance, anticipated graduation date
- Degrees and awards received
- Most recent previous educational institution attended by the student

Confidential Indicator – Banner flag which indicates the student requests that no information should be released about this student to a third party. **Any violation of privacy may subject offenders to disciplinary action.**

Employee Data

By North Carolina statutes, the University is required to treat personal information about all its employees as confidential. The University expects all personnel granted access to personal employee information, in order to carry out the functions of their job, to strictly protect the confidentiality of information to which they may have access and to abide by this policy. **Any violation of privacy may subject offenders to disciplinary action.**