

Barton Financial Aid Employee Confidentiality/Non-Disclosure Agreement

I (Barton employee) have reviewed and understand the following statements:

- All Barton student and employee records are considered confidential.
- I have an ethical and legal obligation to protect all confidential information used or obtained in the course of performing my duties and I understand that all policies on confidentiality apply equally to data stored on the computer and on paper records as well as information discussed.
- I will only access information that I need for my job.
- I will not access, show, tell, use, release, e-mail, copy, photograph, give, sell, review, change or dispose of any information **unless it is part of my job**. I.e., authorized shredding of confidential papers
- Unauthorized use of, or access to, confidential information may result in discipline up to and including termination.
- My supervisor has explained departmental confidentiality/non-disclosure policies to me and the consequences of non-compliance.
- Work will be monitored for appropriate use or inappropriate access. Confidentiality violations will be reported immediately. All staff and employees are responsible for immediately reporting any apparent violations of this confidentiality policy to their supervisor.
- When my work at the College ends, I will not disclose any confidential information and I will not take any of this information with me if I leave or am terminated.
- I will keep my computer password secret and I will not share it with anyone.
- I will log out or secure my workstation when I leave my work area.

Examples of Confidential Information: Such as, but not limited to (1) Social security number; (2) Birth date; (3) Home phone number; (4) Home address; (5) Student grades; (6) Gender; (7) Ethnicity; (8) Courses taken; (9) Student schedule; (10) Test scores; (11) Advising records; (12) Educational services received; (13) Student ID

Examples of Breaches of Confidentiality: (1) Unauthorized reading of student and employee information; (2) Accessing information on family, friends, or co-workers; (3) Telling someone your password so that he or she can log in to your account; (4) Making unauthorized marks on student and employee paperwork; (5) Making unauthorized changes to a student or employee file; (6) Discussing confidential information in a public area, such as hallway, cafeteria, etc. (7) Being away from your computer while you are logged into an application; and (8) Allowing someone to access confidential information using your password.

Employee Signature Section

Printed

Name: _____ Signature: _____ Date: _____