Employee Confidentiality

The College adheres to the Family Educational Rights and Privacy Act (“FERPA”), a federal law enacted in 1974 that provides safeguards regarding the confidentiality of student records. All employees of the College are expected to be familiar with the basic provisions of FERPA to ensure that they do not violate federal law. Details of FERPA are included in the Student Records Policy. (Appendix B Student Handbook or Policy 601-02-07AP)

Each employee is expected to sign the following agreement, prior to beginning work:

Employee Confidentiality Agreement

I understand that all information gained from student and/or employee files (including computer generated documents) or heard in the course of my employment is strictly confidential. I will not share this information with anyone other than with those authorized to receive the information or as mandated by provisions in state or federal law.

I will not acquire or seek to acquire confidential information about students and/or employees, including information contained in student or personnel files, unless the information is needed and is essential to perform my job duties. I will not reveal information about students that I may learn or have learned while performing my job.

I understand that even a minor disclosure of information, e.g., disclosing a student’s class schedule, may be a violation of FERPA and/or College policy and could result in disciplinary action, up to and including the loss of my job.

I understand that anyone having access to the college's data information systems is not allowed to leave campus with any information obtained from the college's data information systems by means of any storage device such as flash drives, cloud storage, cd/dvd, external hard drives, or any kind of paper form of the information.

I understand that I can only use the College's equipment to access the college's data information systems. This data can only be printed to a network printer or saved to the College's network drive.

I agree that files with protected information or other documents in print or electronic format will not be left unattended in public areas for others to view, and that no files or copies of records in any format will leave this office/department without proper authorization.

I understand that computer passwords that may be provided will not be shared with anyone other than those authorized. I will ensure the electronic devices that I use, or for which I am responsible, are properly secured when not in use.

I agree to abide by the guidelines and procedures of the College in accepting credit card payments on behalf of college in the course of my employment. Guidelines are established by the President for which will remain in compliant with those set by the Payment Card Industry (PCI).

I have read and understand my responsibilities as stated in this agreement and understand that any violation of this policy or other policies related to the appropriate release or disclosure of information will result in disciplinary action up to termination of my employment and/or legal sanctions.

Guidelines and Procedures for Accepting Credit Card Payment

(Mandated by Payment Card Industry (PCI))

1. Credit Card Information (Cardholder Data) is obtained from customers only for business purposes and only with cardholder consent.
2. The full credit card track number, including the 3 digit security code, is never solicited or kept.
3. Credit cardholder data should never be kept in a ‘shadow’ database such as an Excel spreadsheet.
4. Merchant receipts (receipt kept by college) should not have full card number – only the last 4 digits should be displayed. If credit card merchant service provider cannot eliminate the full card number on the merchant receipt, then the merchant receipt should be handled same as cash (i.e., locked in safe, never left unattended) and should be shredded when no longer needed.
5. Cardholder data collected from phone-in sales should be destroyed by shredding immediately after the sale is processed and credit cards are settled.
6. Cardholder data should never be E-mailed, faxed, or mailed (US or Intercampus) in an unsealed envelope.
7. Credit card sales should be settled at least once daily.
8. Access to cardholder data is on a need-to-know basis only. Supervisors are to determine who in your area has a need to access this information.
9. Any suspected security breach (files that appear to have been tampered with, lost or stolen keys or passwords, etc.) should be reported to the Controller immediately.
10. Passwords should be changed regularly.
11. Misuse of credit card information is punishable to the full extent of the law.

Policy Number: 306-02-02BP

Adopted: May 11, 2010

Amended: May 24, 2011; January 27, 2015

Employee confidentiality agreement

Download a PDF of this policy