



Technology Confidentiality Agreement

Required fields are marked with an *

Recognizing the need to maintain individual and institutional rights to privacy and confidentiality and realizing that, as an employee of Desert Community College District, my assigned responsibilities necessitate the handling of sensitive information about employees, students and graduates, I affirm my intention to preserve the strictest standards of confidentiality in the use of District Information Systems.

I will use Colleague, CANVAS, WebAdvisor, Informer, Galaxy and all other data entry and data reporting software only for the purposes for which I am authorized.

I will not disclose any of my LOGIN ID's or passwords to any person.

I will not allow anyone else, even other authorized users, use of my PC while it is logged on to the District network under my LOGIN ID, nor allow casual onlookers to view privileged information.

I will not participate in unauthorized disclosure of any data or password. I will print records only when necessary.

I will report any attempted or successful violation of institutional or personal security or privacy policies and procedures to my supervisor and the Executive Director, Educational Technology.

I will not establish separate databases which duplicate or conflict with the Colleague system. I will submit updates of data to the appropriate office upon receipt.

If I am authorized to remove the HR Privacy Flag from an employee record, I will only do so in the course of official college business. I will replace the HR Privacy Flag to the employee record immediately after the work has been completed or by the end of the work day.

Any confidential employee or student data archived or printed will be destroyed or shredded after its use.

I understand the intent of this statement and will exercise diligence in performing my duties in accordance with institutional policies. Any unwarranted and deliberate violations of the terms of this agreement may subject me to possible disciplinary action, including termination, and/or legal actions. All data entry fields are tracked to the LOGIN ID and the user with the LOGIN ID may be held responsible for any violation.

Name*:

Department*:

Signature (type or sign)*:

Date*: