Acceptable Use Policy
Access to Computer and Electronic Resource Systems for Third Party Vendors and Contractors

College of the Desert Computer and Electronic Resource Systems

The College of the Desert ("Community College") owns, leases, and/or operates a variety of computer and electronic resource systems, which are provided for the use of District faculty, administrators, staff, and authorized third party vendors and contractors in support of the educational mission and programs of the Community College. Such computer and communication systems include, but are not limited to, electronic mail (e-mail), telephone, voicemail, computer software, and access to the Internet and other wireless Community College networks (collectively, "Community College Network").

Scope of Applicability

This Acceptable Use Policy ("Policy") applies to individuals who obtain authorized access to the Community College Network, including authorized third party vendors, independent contractors, and guests ("Third Parties"). This Policy extends to the use of and access to the Community College Network, including District computer equipment and communication systems and any associated data, which data may constitute protected information. "Protected Information" is defined as confidential information that identifies or is capable of identifying a specific individual, including but not limited to personally identifiable information and other non-public information, student records, individual financial information, or protected health information, that is subject to state or federal laws restricting the use and disclosure of such information.

Terms of Acceptable Use

Except as provided in Board Policies or agreements pertaining to intellectual property rights, Third Parties have no right of ownership in any Community College Networks, or the information they contain by virtue of their access to or use of all or any portion of the Community College Network. By accessing the Community College Network, data, associated systems and information, a Third Party agrees to abide by the following restrictions:

1. All rights, including all intellectual property rights, shall remain the exclusive property of the Community College, and Third Party has a limited, nonexclusive license solely for the purpose of performing authorized obligations at the direction of the Community College.

2. Third Party agrees to comply with any and all applicable state, federal and international laws, as well as best practices, governing the collection, access, use, disclosure, safeguarding, and destruction of Protected Information. Such laws include, but are not limited to, the Family Educational Rights and Privacy Act ("FERPA"), the California Information Practices Act ("CIPA"), Article 1, Section 1 of the California Constitution, and the federal Health Insurance Portability and Accountability Act ("HIPAA").

3. Third Party will not access, use or disclose Protected Information for any purpose other than to carry out the purposes for which Community College disclosed to or allowed Third Party to remotely access the Protected information, except as permitted or required by applicable law, or as otherwise authorized in writing by Community College.

4. Third Party will not change how Protected Information is collected, used, or shared under the terms of this Policy in any way without providing advanced notice to and receiving written consent from Community College.

5. Third Party is prohibited from mining Protected Information for any purposes other than those agreed to by the parties. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited.

6. Third Party agrees to return the Protected Information to Community College within 30 days of the termination, cancellation, expiration, or other conclusion of Third Party's obligations to Community College.

7. Third Party will report any suspected or confirmed Breach[1] to Community College upon discovery, both orally and in writing, but in no event more than two (2) business days after Third Party reasonably believes a Breach has or may have occurred. Third Party's written report shall identify the following information:

    a. the nature of the unauthorized access, use or disclosure;
    b. a list of the types of Protected Information that were or are reasonably believed to have been the subject of the breach;
    c. the date or estimated date of the breach, or the date range within which the breach occurred;
    d. a general description of the breach incident, including the person(s) who accessed, used, disclosed and/or received Protected Information, if known; and
    e. such other information as reasonably requested by CCD.

Failure to Comply

Any Third Party who accesses Community College Networks, associated data and/or Protected Information for unacceptable practices has violated this policy and is subject to disciplinary proceedings including but not limited to suspension of system privileges, termination of employment, and/or legal action to the extent permitted by law. Any disciplinary action taken against a Third Party for violating this policy shall be in accordance with applicable laws, regulations, policies or collective bargaining agreements, if any.

Community College reserves the right to limit or restrict the use of its computing and electronic resource systems based on institutional priorities and financial considerations, as well as when it is presented with evidence of a violation of Community College policies, contractual agreements, or state and federal laws.

Acknowledgement and Agreement

By signing below, Third Party acknowledges receipt of Community College's Acceptable Use Policy and agrees to abide by its terms and conditions as set forth above.

Dated: _____ Signature: _____

Name: _____

Title: _____

[1] "Breach" means an information security event that impacts and/or has the potential to impact the confidentiality, integrity, or availability of Community College's information systems or Protected Information.