CAMPUSLOGIC DATA PROTECTION POLICY

This Data Protection Policy is incorporated by reference in the Terms and Conditions of any executed Subscription Order Form between CampusLogic and Customer. CampusLogic will abide by this Data Protection Policy in every material respect during the Term of Service of any Subscription Order Form for Online Services and thereafter as set forth in any applicable Subscription Order Form. Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the Terms and Conditions.

1. GENERAL

Relationship. As a SaaS company, CampusLogic serves as a data processor for any Customer who uses its Online Services to collect and store sensitive information. Customer fills the role of data owner while CampusLogic and its products act solely as an agent on behalf of Customer. CampusLogic maintains only that information which Customer has asked it to process and processes it only upon, and in accordance with, Customer's direction and instructions.

Scope. This Data Protection Policy covers the collection and use of information for any Online Services provided by CampusLogic for which a Subscription Order Form for Online Services exists between Customer and CampusLogic. This Data Protection Policy does not reflect the practices of Customer, and CampusLogic is not responsible for Customer's data security practices or privacy policies. CampusLogic does not review, comment upon or monitor Customer's compliance with their respective data security policies, nor does CampusLogic determine whether they are in compliance with or conflict with the terms of Customer's published data security or privacy policy.

Modifications. CampusLogic reserves the right to change, modify, add, or remove portions of this Data Protection Policy at any time. All Modifications will be posted on the CampusLogic website and Customers will be notified of such Modifications at least 30 days prior to posting. Modifications will be deemed accepted and become effective 30 days after such notice unless Customer first gives CampusLogic written notice of rejection of the Modification. Customer's continued use of the Online Service following the effective date of a Modification will confirm Customer's consent thereto.

2. CUSTOMER DATA

Ownership of Customer Data. Customer possesses and retains all right, title, and interest in all data in any form collected through any Online Service from (i) Customer's customers including students and parents, (ii) other third parties approved by Customer, or (iii) collected or accessible directly from Customer, (collectively, "Customer Data"). Customer Data, and CampusLogic's use and possession thereof is solely as Customer's agent. Customer may access and copy any Customer Data in CampusLogic's possession at any time. CampusLogic will facilitate such access and copying promptly after Customer's request.

Location of Customer Data. Unless otherwise specified in any Subscription Order Form, CampusLogic hosts all of its SaaS products and provides all of its Online Services at Microsoft managed datacenters located in the United States. Microsoft's Windows Azure ("Azure") runs in geographically dispersed datacenters that comply with key industry standards such as ISO/IEC 27001:2005. Microsoft may transfer Customer Data within the United States for data redundancy, disaster recovery, or other purposes but Customer Data will never be stored outside of the US. For more information, please visit: https://www.windowsazure.com.

Access and Use of Customer Data. Unless it receives Customer's prior written consent, CampusLogic: (i) will not access or use Customer Data other than as necessary to facilitate the applicable Online Services; and (ii) will not give any third party access to Customer Data. Notwithstanding the foregoing, CampusLogic may disclose Customer Data as required by applicable law or by proper legal or governmental authority. CampusLogic will give Customer prompt notice of any such legal or governmental demand and reasonably cooperate with Customer in any effort to seek a protective order or otherwise to contest such required disclosure, at Customer's expense.

Customer Data Retention and Deletion. CampusLogic will retain any Customer Data in its possession until Erased as defined herein. CampusLogic will Erase: (i) all copies of Customer Data promptly after Customer's written request and (ii) all copies of Customer Data no sooner than 60 days and no longer than 120 days after Termination of any applicable Subscription Order Form for Online Services unless otherwise required by law. Promptly after Erasure, CampusLogic will certify such Erasure in writing to Customer. ("Erase" and "Erasure" refer to the destruction of data so that no copy of the data remains or can be accessed or restored in any way.)

Statistical Information. CampusLogic may compile statistical information related to the performance of the Online Services, and may make such information publicly available, provided that such information does not incorporate any Customer Data and/or identify any Customer Confidential Information or include any Customer's name related to such information. CampusLogic retains all intellectual property rights in such information.

3. EMPLOYEES

CampusLogic Employees. CampusLogic will not allow any of its employees to access Customer Data, except to the extent that an employee needs access in order to facilitate the applicable Online Services, including quality assurance, in any Subscription Order Form, with CampusLogic agreeing to comply with CampusLogic's obligations set forth in this Data Protection Policy. CampusLogic will perform a background check on any individual to whom it gives access to Customer Data. Such background check will include, without limitation, a review of the individual's criminal history, if any. CampusLogic will not grant access to Customer Data if the background check or other information in CampusLogic's possession would lead a reasonable person to suspect that the individual has committed identity theft or otherwise misused third party data or that the individual presents a threat to the security of Customer Data.

4. COMPLIANCE

General Compliance. CampusLogic will ensure that all Online Services are compliant with all applicable laws and regulations, under federal, state, local laws and regulations in every material respect. To the extent that such regulations apply to any Online Services, CampusLogic will comply with (i) 16 CFR Part 314, "Standards for Safeguarding Customer Information" and (ii) handling, processing, security and protection of confidential information which is "non-public personal information" (as defined in the Gramm-Leach-Billey Act) and other requirements that are specifically required of an educational institution under the Federal Trade Commission's Privacy of Consumer Financial Information and/or Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 CFR Part 99).

5. SECURITY

Security Features. Every User of every CampusLogic SaaS product must have a valid username and password combination. Passwords are User-generated and not known by any employee of CampusLogic. In addition to feature-level security, CampusLogic employs fine-grained data level security to limit access to data by User type. CampusLogic uses industry-standard 256-bit secure socket layer (SSL) technology and digital certificates to encrypt and authenticate transactions. Access to the database is controlled by and limited to the applicable CampusLogic SaaS application only. Employees of CampusLogic do not have physical access to the database or data. Additionally, all data changes are logged and audited.

Security Testing & Audits. CampusLogic's data center receives an annual audit against the Service Organization Control (SOC) reporting framework for both SOC 1 Type 2 and SOC 2 Type 2. These audits examine controls related to security, availability, and confidentiality. Audits are conducted in accordance with the Statement on Standards for Attestation Engagements (SSAE) No. 16 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3402 put forth by the International Auditing and Assurance Standards Board (IAASB). In addition, the SOC 2 Type 2 audit included an examination of the Cloud Controls Matrix (CCM) from the Cloud Security Alliance (CSA). Audit reports are available to Customer upon written request.

Security and Breach Notification. CampusLogic will promptly notify Customer of any actual or potential exposure or misappropriation of Customer Data (any "Breach") that comes to CampusLogic's attention. CampusLogic will coordinate with Customer to Users in the event of any break-in or attempted break-in to the Online Services, security protocols, network(s), or data centers(s) which contain personal financial records of the Users. CampusLogic shall report any confirmed or suspected breach to Customer upon discovery, both orally and in writing, but in no event more than two (2) business days after CampusLogic reasonably believes the breach to have occurred, unless CampusLogic is otherwise prohibited by other applicable law from providing such notice to Customer. CampusLogic's report shall identify: (i) the nature of the unauthorized access, User or disclosure; (ii) the protected information accessed, used or disclosed; (iii) the person(s) who accessed, used and disclosed and/or received the protected information (if known); (iv) what CampusLogic has done or will do to mitigate the deleterious effect of the unauthorized access, use or disclosure; and (v) what corrective action CampusLogic has taken or will take to prevent future unauthorized access, use or disclosure. For California Customers and Users, CampusLogic will cooperate with Customer in complying with the notification requirements of California Civil Code sections 1798.29 and 1798.82.

Questions regarding this Data Protection Policy should be directed to privacy@campuslogic.com or our corporate offices at 1325 N. Fiesta Blvd, Suite 102, Gilbert, AZ 85233.