MTC Privacy and Security

Last updated July 16, 2021

01. Data Storage and Data Access
   a. Application and data all stored in Google Cloud.
   b. Information is stored inside the USA.
   c. All data at rest is encrypted using Google's "wrapped key" key encryption key method and encrypted at the storage level using AES-256.
   d. Data is not shared, sold, or mined with or by a third party.
   e. Data in transit is protected by HTTPS.
   f. Application is multi-tenant where each member school has a separate school account in which data and access is completely siloed from another school's account.
   g. Access to information stored or processed by the application is limited to: school user(s) who are granted accounts to the system, as designated by the member school administrator, and a limited number of MTC super administrators, for support purposes.
   h. Background checks are performed on personnel with administrative access to servers and School System data.
   i. School user account access is controlled through the expiration date which is set by the administrator of the school account. School user accounts can also be immediately suspended or deleted by the administrator of the school account.

02. Availability
   a. Automated backups of the database are made daily and retained for the last 30 days.
   b. Google Cloud load balancing provides protection against denial-of-service attacks.

03. Audits and Security Standards
   a. Mastery Transcript Consortium complies with the International Organization for Standardization (ISO) security standard.
   b. Mastery Transcript Consortium complies with Family Educational Rights and Privacy Act (FERPA) and Children's Online Privacy Protection Act (COPPA) data security standards.