Data Security and Privacy Plan - Ed law 2d

This Data Security and Privacy Plan applies to the use by the School or District of the products provided by Prodigy Education Inc. ("Prodigy").

Prodigy agrees that it will protect the confidentiality, privacy and security of the Student and/or Protected Data received from a School or District in accordance with the applicable Parents Bill of Rights for Privacy and Security. "Student Data" means personally identifiable information from the student records of the School or District that Prodigy receives from through the use of its products. "Protected Data" means Student Data.

Additional elements of Prodigy's Data Security and Privacy Plan are as follows:

a) In order to implement applicable state, federal and local data security and privacy requirements, Prodigy will review its data security and privacy policy and practices to ensure that they are in conformance with applicable federal, state and local laws and the terms of any agreements with Schools/Districts. In the event that Prodigy's policy and practices are not in conformance, Prodigy will implement commercially reasonable efforts to ensure such compliance.

b) In order to protect the security, confidentiality and integrity of Protected Data received from Schools/Districts, Prodigy will have the following reasonable administrative, technical, operational and physical safeguard and practices in place:

http://www.prodigygame.com/main-en/privacy-policy/

Prodigy's data is stored in the cloud, on Amazon Web Services (AWS) as we use AWS to host our infrastructure, with servers based in Virginia, USA. We follow the following security best practices -

- Data stores are segregated into private subnets which have restricted network access.
- Disk storage and transport is encrypted using industry standard encryption.
- Backup access is restricted to select team members and audited
- Secrets are stored encrypted, access to them is restricted and usage is by injection into applications at run time.
- All data layer access is audited via industry standard tooling.

The security protections taken to ensure data will be protected that align with the NIST Cybersecurity Framework and industry best practices include:

- Annual security awareness training to ensure the security and confidentiality of student records.
- SSL encryption - Prodigy protects any information transferred through our website by encrypting it with the Secure Socket Layer (SSL) protocol by default. This makes it more difficult for malicious third parties to intercept user information.
- Independent service-level APIs - Students' PII is only available through a select few APIs. This minimizes the impact of a potential breach of any individual API.
- Database protection - Prodigy's databases are inaccessible to all IP addresses except for a pre-specified list of whitelisted IP addresses. All databases are also password protected.
- Periodic data review - Our team periodically reviews our data collection, storage, and processing policies and practices against leading industry standards to ensure that we are compliant.
- Infrastructure Security - Prodigy segments network topology to restrict access to the data storage layer to a limited subset of employees and we follow the best security standards.

Prodigy manages data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Prodigy will provide prompt notification to School or District of any breaches or unauthorized disclosures of Protected Data.

Prodigy agrees to incorporate the requirements of the New York Parent's Bill of rights for data security and privacy, to the extent that any of the provisions in the Bills of Rights apply to Prodigy's possession and use of Protected Data.