Always Learning

Last Updated: January, 2023

Dream See Do: Data & Security Protocols

Overview

Dream See Do strives to offer a secure and private space for people to learn in. We adhere to the principle of least privilege in terms of data and systems access, and use best practices and well-tested, open-source technologies when possible.

What security do we use to protect learner data?

We use bank-level encryption: data is encrypted at rest with AES-256, block-level storage encryption. All access to data is governed by the administrators of the course. The data is housed in ISO 27001-compliant data centers with strict physical security. We complete penetration testing by an external vendor. Third-party vendors do penetration and vulnerability assessments.

How do you ensure data continuity and uptime?

We have continuous database backups, and also maintain daily and weekly backups offsite. We use cloud hosting to ensure that we can offer the maximum uptime possible, and try to minimize any single points of failure in our system configuration.

What PII information can learners share with the platform?

They can create their own profile, and can choose what information they would like to share (the only required field is email and name). They can join a private group solely dedicated for their training(s).

They can share reflections as they learn in text or video, and can choose their own privacy settings for each response (if they want to keep it private, or share with their private group).

How do you handle data deletion?

We are GDPR-compliant. As a result, individual learners can delete their account and all of their responses and personally-identifiable data. We can also delete the entire cohort's data for clients at once in response to any data deletion requests.

We do keep some anonymized usage data to improve our system’s design and usability.

More Information

Our Privacy Policy is located here: https://www.dreamseedo.org/help/privacy_policy

NYS EDU Department Section 121 Topics

How will state, federal and local data security and privacy requirements be met?
To understand our approach, please refer to our general data & security protocols that we adhere to: [link]

We always operate from the principle of least privilege, and so only a very limited number of staff on our team have access to any PII (the majority are technical/engineers). We only share any information with our subcontractors that is materially necessary, and do so in a way that it cannot be linked to customer accounts (e.g. they may have access to an IP address, and not any further identifiable information).

We only work with adults (teachers and administrators) and do not allow clients to offer student access to the platform, to reduce our exposure. We also strongly encourage that no student data be shared on the platform.

How will administrative, operational and technical safeguards be in place to protect PII?
We are already GDPR compliant, which means that we have implemented everything necessary to protect personally-identifiable information:

- Administrative safeguards such as security training and limiting access to PII using time-bound access tokens/credentials.
- Operational safeguards such as always internally communicating using direct, secured communication tools.
- Technical safeguards such as encrypting all data at rest, logging all data processing activities, and regular data and access audits.

How will you maintain compliance with requirements of Section 121.3(c)?
The criteria identified here is basically the same as our existing data protection and privacy compliance. The only exception is requirement #4: Any challenges to the accuracy of teacher or principal data can be sent to our support team via email: support@dreamseedo.org.

How will officers/employees receive training on federal and state laws prior to gaining access to PII
All existing employees have received online security training on data protection and safeguards. We will brief any new employees during their onboarding process with any specifics related to NYS EDU Section 121, in addition to other national and state-specific regulations, such as FERPA and California's CCPA.

Will sub-contractors be used, and how are those relationships maintained to ensure PII is protected?
We do use subcontractors, although only a few have access to any PII. The only one with full access is our website hosting provider (Heroku/AWS), who maintain ISO

27001-compliant data centers. We have signed data protection agreements with all subcontractors.

How will data security and privacy incidents be managed?
If we learn about any breaches of our systems, we will simultaneously and expeditiously work to both secure access, as well as send email notifications to those who may be affected, within 1 business day of the incident, unless we are in any way legally restricted from doing so.

How will data be returned to the educational agency when the contract is terminated or expired?
Data will not be returned to the educational agency. Instead, it will be deleted when the contract is terminated or expires.