Data Security and Privacy Plan

1. Exclusive Purposes for Data Use
    a. Please list the exclusive purposes for which the student data [or teacher or principal data] will be used by the service provider.

Data will be used for the purposes of Authentication and Authorisation only, in order to provide access to Digital Theatre+ via your Identity Provider.

Digital Theatre will use your data only to provide the Services and as otherwise permitted by this Agreement and the Privacy Policy located at: https://edu.digitaltheatreplus.com/privacy-policy

Initial NM

2. Data Accuracy/Correction Practices
    a. Parent [student, eligible student, teacher or principal] may challenge the accuracy of the data by…

Data is send from your Identity Provider, so correction of information occurs within your own Identity Management System.

You shall have sole responsibility for the accuracy, quality, reliability, integrity, and legality of Your Data. You have the right to demand rectification of inaccurate Personal Data about you. You can request this via https://support.digitaltheatreplus.com

Initial NM

3. Subcontractor Oversight Details
    a. This contract has subcontractors: Yes ☑ No ☐
    b. Describe how the contractor will ensure subcontractors abide by data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations:

Student data is stored in our Identity Platform - a tenant in Okta - in the continental US. Student data is encrypted at rest and in transit (using at least TLS v1.2) using keys and certificates unique to DT+. No data is removed from the DT+ Okta instance for any purpose at any time. Data is used for the purpose of authentication only. Data is collected on login. Data is deleted 14 months after last login. Access to student data is limited to customer success and developer staff, who have had criminal records background checks. Each customer's data is logically separated at the application level, preventing any cross-access between different customer datasets. Amazon Web Services (AWS) provides the infrastructure that hosts Okta's identity-as-a-service platform (IDaaS). DT+ specific cryptographic keys are protected using the AWS KMS service and a FIPS 140-2 Level 2 certified hardware security module with Level 3 physical protection.

Initial NM

4. Security Practices
    a. Where is the data stored? (described in such a manner as to protect data security)
    Student data is stored in our Identity Platform - a tenant in Okta - in the continental US.
    b. The security protection practices taken to ensure data will be protected include:

Student data is stored in our Identity Platform - a tenant in Okta - in the continental US. Student data is encrypted at rest and in transit (using at least TLS v1.2) using keys and certificates unique to DT+. No data is removed from the DT+ Okta instance for any purpose at any time. Data is used for the purpose of authentication only. Data is collected on login. Data is deleted 14 months after last login. Access to student data is limited to customer success and developer staff, who have had criminal records background checks. Each customer's data is logically separated at the application level, preventing any cross-access between different customer datasets. Amazon Web Services (AWS) provides the infrastructure that hosts Okta's identity-as-a-service platform (IDaaS). DT+ specific cryptographic keys are protected using the AWS KMS service and a FIPS 140-2 Level 2 certified hardware security module with Level 3 physical protection.

Initial NM

5. Contract Lifecycle Practices
    a. The agreement expires 06/30/2024
    b. When the agreement expires,
        i. How long will the student [or teacher or principal] data be retained?
        Data is deleted 14 months after last login.
        ii. How will the student data be disposed of?
        Data is deleted 14 months after last login.

Initial NM

6. Encryption Practices
    a. Data encryption is applied in accordance with Education Law 2-d 5(f)(5)
    Yes ☑ No ☐ Initial NM

7. Training Practices
    a. Annual training on federal and state law governing confidentiality is required for any officers, employees, or assignees who have access to student [or teacher or principal] data
    Yes ☐ No ☑ Initial NM

Digital Theatre (US) LLC
Company Name

Nick Myers, Director of Technology
Print Name and Title

N Myers
Signature of Provider

02/01/2024
Date