ASPIREDU
EDUCATIONAL ANALYTICS

# Data Retention and Security Policy

September 2024

**Purpose**

This document defines the data security policy of AspirEDU, Inc as it is related to its solutions, Dropout Detective and Instructor Insight. AspirEDU takes the privacy of its clients and their students very seriously.

**Intent**

The goal of this policy is to inform clients of AspirEDU of the procedures relating to data security compliance.

The data covered by this policy includes, but is not limited to, all electronic information found in databases, applications, and other media.

**Data Types**

AspirEDU deals with three main kinds of data:

1. **Student LMS data** that relates to data brought into Dropout Detective through API calls to the LMS. This includes data such as grades, ID number assigned by the LMS, and assignment data.
2. **Computed data** that is calculated based on the Student LMS data referenced above. This includes data such as student risk scores.
3. **Application data** that is used to access LMS APIs and for users to access Dropout Detective. This includes data such as API tokens and Dropout Detective usernames/passwords.

**Data Retention Policies**

AspirEDU has different retention policies for each type of data. Some are subject to client approval and input.

1. **Student LMS data** is retained for the entire term of our contractual relationship, unless otherwise documented. This allows access to previous points in time for comparisons. Once the term/retention period expires, that data will be permanently deleted by AspirEDU.
2. **Computed data** is retained for a minimum of five (5) years. This allows the ability to look back across a student's time with the client to compare risk scores.
3. **Application data** is retained for the entire term of our contractual relationship. Once the term/retention period expires, that data will be permanently deleted by AspirEDU.

**Data Access Policies**

Currently, the developers and administrators of Dropout Detective for AspirEDU have access to all three types of data. Passwords are encrypted and cannot be read or reverse-engineered by AspirEDU staff.

AspirEDU staff is not permitted to copy client data to mobile devices, external media or e-mail it to addresses other than AspirEDU staff addresses.

**Server Security**

AspirEDU data is stored on the AWS technology platform. For more detailed information, please see the documents describing “Amazon Web Services – Security Documentation”; these will be provided upon request.

**Password Policy**

Passwords used by AspirEDU staff to access the system are at least 12 characters long, including at least one numeric character and one non-alphanumeric symbol.

**Change Management**

All changes to the AspirEDU system undergo review by a staff member other than the person who created the change. Once reviewed and tested, the change is pushed to production on a regularly scheduled basis.

Emergency changes, necessitated when there is an issue within the system that is adversely affecting its use, may be pushed to production on a non-scheduled basis but undergo review normally as scheduled changes do.

**Management**

Ownership of this policy falls to the Chief Technology Officer ("CTO"). Questions about this policy, or reports of misuse of corporate or personal data, should be directed to security@aspiredu.com. The CTO will maintain data access privileges, which will be updated as required when an employee joins or leaves the company.

**Review**

Management is responsible for keeping this policy current. This policy will be reviewed annually or as circumstances arise.

**Response to Security Incident**

In the case of an incident where the security of the system has been compromised, AspirEDU will determine the extent of the breach and communicate same to the affected clients within 72 hours of discovery of the breach.

**Right to Erasure**

Upon notification of an individual who wants to have their data erased from our system, we will erase the data within 30 days.