Admicity Data Security and Compliance Policy for Student Information Integration

Version:	1.0.0
Date of version:	2024-02-28
Created by:	Volodymyr Kozel
Confidentiality level:	Sensitive

CHANGE HISTORY

Date	**Version**	**Created by**	**Description of change**
2024-02-28	1.0	Volodymyr Kozel	Base document

TABLE OF CONTENTS

Admicity

Data Security and Compliance Policy

1. Introduction

This document outlines the data security measures implemented within Admicity to ensure the protection and confidentiality of student information imported from school infrastructure. As part of our commitment to data security and compliance, this document details the safeguards in place to mitigate risks and maintain the integrity of student data.

2. Data Collection and Processing

Purpose of Data Collection: Admicity collects student information from school infrastructure to exchange the data between parents and the school.

Types of Data Collected:

- Student names
- Contact information (e.g., email addresses, phone numbers, home address)
- Medical and SEN information
- Dietary needs
- Ethnicity
- Welfare

Methods of Collection: Student data is imported securely from school infrastructure (SIMS application) using encrypted connections and authenticated APIs.

Legal Basis for Processing: The processing of student data is based on contractual agreements with the schools and compliance with relevant data protection regulations, including the Family Educational Rights and Privacy Act (FERPA).

3. Data Storage and Security

Storage Location: Student data is stored securely in encrypted databases hosted on AWS servers in the eu-west-2 region (London) and, therefore, falls under the regulation of UK legislation. Access to the AWS console, which hosts all services, is protected by a strong password and multi-factor authentication (MFA) and has different access rights for administrative users. The service is available 24/7. Administrative access to all cloud services (EC2 and RDS) is limited by security groups and is allowed only for specified IP addresses and services.
The application servers use the latest operating system versions with security updates and the latest software. Access to servers from the Internet is limited by the SSH protocol for certain IP addresses. It is possible only with a private key (without the possibility of remote password login). Access to the database is also restricted.

Data Encryption: All student data, both at rest and in transit, is encrypted using AES-256 encryption algorithms.

Access Control: Access to student data is strictly controlled through role-based access control (RBAC), with access granted only to authorised personnel with a legitimate need for accessing student information.

Data backup policy: an automatic backup is configured for the database with a backup retention time of 7 days. The data is encrypted and stored exclusively in the cloud service in the eu-west-2 region (London).

4. Data Retention and Disposal

Retention Period: Student data is retained only for the duration necessary to fulfil the purposes outlined in the project's agreement with the schools.

Data Disposal: Upon expiration of the retention period or request from the schools, student data is securely deleted from the project's databases using industry-standard data disposal methods.

5. Data Access and Auditing

Access Logs: Access to student data is logged and monitored to track all interactions with the data, including access, modifications, and deletions.

Audit Trails: Audit trails are maintained to record and trace all activities related to student data processing and access for accountability and transparency purposes.

6. Data Breach Response Plan

Reporting Procedure: In the event of a data breach or unauthorised access to student data, the project will promptly notify the schools and relevant authorities following legal requirements and contractual agreements.

Investigation and Remediation: An incident response team will conduct a thorough investigation to assess the scope and impact of the breach and take appropriate remedial actions to mitigate further risks and prevent future occurrences.

7. Conclusion

Admicity team is committed to maintaining the highest standards of data security and confidentiality in the handling of student information imported from school infrastructure. By implementing robust data security measures and adhering to regulatory requirements, we strive to ensure the privacy and integrity of student data at all times.