# Equal Opportunity Schools

## Data Privacy Overview

EOS is committed to data security and privacy. We take very seriously our legal and ethical standards in our management of all information that might be considered sensitive. This document provides an overview of key confidentiality and security practices at Equal Opportunity Schools.

All individuals at Equal Opportunity Schools who have access to our data have undergone background checks and executed the EOS Confidential Information Agreement, which helps ensure both personal and organizational accountability to our standards.

Data is housed on Amazon EC2, which works in conjunction with Amazon Virtual Private Cloud (VPC) servers. Users access data through a proprietary EOS application. This application is secured with HTTP (HTTPS) encryption. Access to our application and data is controlled through an internal EOS approval process managed by the Director, Database & Product Development.

EOS computer hard drives are encrypted using Microsoft BitLocker Encryption technology. School and district personnel inputting and/or accessing data through our secure portal, must agree to and adhere to our Acceptable Use Policy.

At EOS we assign all data to the following security categories, each with the following associated standards:

1. **Highly-sensitive information – information that EOS does not store and that EOS will not accept from schools. If school or district personnel were to accidentally transmit such data to EOS, it would be recognized and destroyed, with a reminder sent to the school or district contact that EOS does not accept highly-sensitive information. Information in this category includes such things as social security numbers.**
2. **Confidential information – FERPA protected student level information and staff data that school or district personnel are authorized by agreement to share with EOS is stored in on a secure database accessible through the EOS Portal.**
3. **Non-confidential information – De-identified and aggregated student and staff data that can be used to understand classroom-level and school-level issues. Schools may authorize or refuse the release of school information to others outside the school at their discretion.**

In implementing the above-described policies, EOS recognizes the obligation of schools and districts to comply with FERPA and state and local policy, and aligns its written agreements with the educational agency accordingly.

**References:** Amazon Web Services Security Center | Microsoft BitLocker Drive Encryption | FERPA Regulations