WHITEBOX
LEARNING
A Flinn Scientific Company

Privacy and Security Policy

WhiteBox Learning holds the privacy and security of our subscribers and students as one of its highest priorities. This privacy policy describes our alignment with the Family Educational Rights and Privacy Act (FERPA) and the NIST Cybersecurity Framework. Specifically, we address what information is gathered and how our processes identify, protect, respond to, and recover from data security and privacy threats.

FERPA and the Parent's Bill Of Rights

The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records. The intent of the law is to provide parents with assurances that sensitive information about their children will be protected. WhiteBox Learning takes this mandate seriously and the remainder of this document provides details about what information is collected and how it is managed. With that said, parents and schools using WhiteBox Learning should take comfort in the fact that the only personally identifiable information (PII) we collect is a student name and optionally, an email address. Student email addresses are only required when a school chooses to integrate WhiteBox with a third-party learning management system (LMS) like Clever and OneRoster. Both forms of PII are considered "directory information" by FERPA and therefore would not generally be considered harmful or an invasion of privacy if disclosed.

To assess WhiteBox Learning processes in the context of student privacy, it is helpful to think of a WhiteBox Learning application as a single project. In other words, the application is not a course. It is a single assignment. Furthermore, the information we collect about how a student uses that project is intended to help instructors improve the learning process. It is entirely the instructor's responsibility to synthesize the information we provide along with their own objective and subjective observations to calculate a grade on the project. Thus, WhiteBox Learning does not even capture or store a project grade, let alone a course grade. We certainly don't have any need to capture or store more sensitive information like attendance, social security numbers, medical records or other forms of data that might cause concern for parents. As far as student privacy is concerned, we do not believe a data breach would be any more harmful than if an ungraded project with a student name were found by someone other than the instructor.

What Information is collected?

Instructors are required to provide email, name, billing address, phone, and organization (school name). This information is necessary so that we can 1) set up an account for you which will allow you to access the Teacher Control Center (TCC) and all purchased applications, 2) send emails to reply to any questions you may have, and 3) in rare cases, we may need to send you information about scheduled application server maintenance or other support matters.

Students gain access to secure application servers using a password protected ID provided to them by the instructor. We collect information about the student's session such as time on task, quiz scores, and other engineering performance data. This information is collected and organized to help the instructor make observations to improve the learning process. To that end, the instructor may optionally enter student names in their Teacher Control Center. When a school chooses to integrate WhiteBox Learning with a third-party LMS like Clever or OneRoster, the school must provide a student email address.

WhiteBox Learning does not sell or share any instructor or student information to outside companies for any reason.

Data Retention

Teacher and student data is the only information gathered. Once a school subscription expires, this data is archived on WhiteBox Learning's secure servers for one year in the event the school re-subscribes and wants access to the stored data. After one year, the data is permanently deleted. If the school desires this information to be deleted sooner, the school can email support@whiteboxlearning.com and type "delete stored data" in the subject area and include the Group ID that was issued by WhiteBox Learning.

If the school has an active subscription, the instructor controls the data. The instructor can choose to delete a classroom and all associated data or archive the classroom, which leaves all associated data available for retrieval at any time by simply unarchiving the classroom.

Security

While the potential harm to student privacy is quite low, protecting student data for the purpose of maintaining the integrity of the experience is critically important to us. Thus, we have a multitude of processes in place to identify, protect, respond to, and recover from data security and privacy threats.

Data Transfer Over the Internet

WhiteBox Learning uses Secure Sockets Layer (SSL) to protect our web sites and user data. SSL is a protocol for enabling encryption on the internet and for helping web site users confirm the owner of the web site.

Storage

All data is stored and encrypted at rest on secure servers located in a secure datacenter managed by Aptum Technologies. Aptum has managed, optimized, and secured data infrastructure for over 20 years and over 25,000 customers. Their technical teams remain current and fully certified, with more than 150 certifications across cloud, network, and infrastructure technologies.

Backups

We are contracted with Aptum for Managed Tivoli Backups. Server hard drives are backed up daily and stored for 30 days on a physically separate, secure machine at the Aptum datacenter.

Firewalls

We are contracted with Aptum for the Juniper SRX 300-L-M firewall. This service provides around-the-clock monitoring and management of our security perimeter which includes several key features.

- The firewall provides defense against denial-of-service attacks and blocks malicious applications and data from access to our network.

- Aptum is contracted to monitor and proactively notify us on critical alerts that relate to the availability, health and performance of the firewall including immediate or potential failures.
- The Aptum Data Service Assurance team, staffed 24/7/365, will notify us of any critical alarms.
- The Aptum Incident Management team ensures normal service is restored as soon as possible when there is an interruption to a device or a reduction in the quality of service.

Disaster Recovery

In the event of a server-down condition where all data on the original server has been lost, Aptum will build a new server to the specifications of the original server plan at a minimum and restore all backed up data to an alternate directory. In addition to the Tivoli data backups, our contract with Aptum includes the Cristie bare metal recovery service. Together, these services enable a rapid recovery process.