Protecting Student Privacy

this page has been moved to https://support.goalexandria.com/knowledge-base/protecting-student-privacy/

Protecting the privacy of students is one of our top priorities, which is why we have multiple policies and practices in place to ensure that happens. In addition to that, there are several things districts and schools should do to bolster student protection.

How does COMPanion protect privacy?

- Ownership and control of data is maintained by districts, not COMPanion.
  - Districts create and control their own procedures.
  - Districts control their employees' access to data.
- COMPanion complies with the Children's Online Privacy Protection Act (COPPA), Family Educational Rights and Privacy Act (FERPA), and New York State's Section 2-D. As districts maintain control over their own data, it is their responsibility to ensure compliance on their end.
- COMPanion will only access confidential data for the purpose of providing client-requested support and will only log in to a client's database with the client's express permission.
- We do not share information or data.
- Daily backup data is kept for a minimum of seven (7) days. If a contract is discontinued, COMPanion destroys all data.
- Communications between Cloud Hosted districts and our servers are safe and secure (https).

What should districts and schools do to protect privacy?

- Comply with the Children's Online Privacy Protection Act (COPPA) and Family Educational Rights and Privacy Act (FERPA). While we advise compliance on your end, ultimately that is your responsibility.
- Follow our Security Best Practices.
- Make sure staff and students use strong passwords.
- Set up your Security properly.
  - Ensure each security group has the correct security level.
  - Ensure each user belongs to the correct security group.

For more information, see our full Terms of Service & Privacy Policy. Specifically, you may want to review sections 5, 12, and 13.