Security Questions to Ask of An Online Service Provider

It is important to understand your provider's security practices to ensure that data shared with and collected by the provider remain private and protected. You should work with your School System's security point of contact to determine whether the security practices of the provider comply both with School System policies and applicable laws. While neither FERPA nor COPPA prescribes specific security standards, school systems should look to industry suggested practices when assessing an online service provider.

The following is a non-exhaustive list of key security questions to discuss with your provider. A service level agreement (SLA) should include as many of these considerations as possible.

Data Collection

- What data does the provider collect?
- What, if any, data is collected by 3rd parties (e.g., via cookies, plug-ins, ad networks, web beacons etc.)?

Network Operations Center Management and Security

- Does the provider perform regular penetration testing, vulnerability management, and intrusion prevention?
- Are all network devices located in secure facilities and under controlled circumstances (e.g. ID cards, entry logs)?
- Are backups performed and tested regularly and stored off-site?
- How are these backups secured? Disposed of?
- Are software vulnerabilities patched routinely or automatically on all servers?

Data Storage and Data Access

- Where will the information be stored and how is data "at rest" protected (i.e. data in the data center)?
  - Will any data be stored outside the United States?
  - Is all or some data at rest encrypted (e.g. just passwords, passwords and sensitive data, all data) and what encryption method is used?
- How will the information be stored? If the cloud application is multi-tenant (several districts on one server/instance) hosting, how is data and access separated from other customers?
  - FERPA requires that records for a school be maintained separately, and not be mingled with data from other school systems or users.
- Are the physical server(s) in a secured, locked and monitored environment to prevent unauthorized entry and/or theft?
- How does the provider protect data in transit? e.g. SSL, hashing?
- Who has access to information stored or processed by the provider?
  - Under FERPA, individuals employed by the provider may only access school records when necessary to provide the service to the School System.
  - Does the provider perform background checks on personnel with administrative access to servers, applications and customer data?
  - Does the provider subcontract any functions, such as analytics?
  - What is the provider's process for authenticating callers and resetting access controls, as well as establishing and deleting accounts?
- If student or other sensitive data is transferred/uploaded to the provider, are all uploads via SFTP or HTPPS?

Data and Metadata Retention

- How does the provider assure the proper management and disposal of data?
  - The provider should only keep data as long as necessary to perform the services to the School.
- How will the provider delete data?
  - Is data deleted on a specific schedule or only on termination of contract? Can your School request that information be deleted? What is the protocol for such a request?
- You should be able to request a copy of the information maintained by the provider at any time.
- All data disclosed to the provider or collected by the provider must be disposed of by reasonable means to protect against unauthorized access or use.
- Upon termination of the contract, the provider should return all records or data and properly delete any copies still in its possession.

Development and Change Management Process

- Does the provider follow standardized and documented procedures for coding, configuration management, patch installation, and change management for all servers involved in delivery of contracted services?
- Are practices regularly audited?
- Does the provider notify the School System about any changes that will affect the security, storage, usage, or disposal of any information received or collected directly from the School?

Availability

- Does the provider offer a guaranteed service level?
- What is the backup-and-restore process in case of a disaster?
- What is the provider's protection against denial-of-service attack?

Audits and Standards

- Does the provider provide the School System the ability to audit the security and privacy of records?
- Have the provider's security operations been reviewed or audited by an outside group?
- Does the provider comply with a security standard such as the International Organization for Standardization (ISO), the Payment Card Industry Data Security Standards (PCI DSS)?

Test and Development Environments

- Will "live" student data be used in non-production (e.g. test or development, training) environment?
- Are these environments secure to the same standard as production data?

Data Breach, Incident Investigation and Response

- What happens if your online service provider has a data breach?
- Do you have the ability to perform security incident investigations or e-discovery? If not, will the provider assist you? For example, does the provider log end user, administrative and maintenance activity and are these logs available to the School System for incident investigation?