PUYALLUP SCHOOL DISTRICT
A Tradition of Excellence

PSD Security Checklist for Online Service Providers – F1 Form

Provider: _____ Phone: _____

Address
_____

Authorized Representative: _____ Email: _____

Key Terms:

FERPA: Family Education Rights and Privacy Act.
COPPA: Children's Online Privacy Protection Act.
PPRA: Protecting Pupil Rights Amendment.
HIPPA: Health Insurance Portability and Accountability Act.
Data: Personal information as outlined by COPPA and personally identifiable information (PII) as outlined by FERPA.
Educational Records: Materials that are maintained by an educational agency or institution or by a person acting for such an agency or institution and contain information directly related to a student.
Online Service Provider: The provider attempting to do business with the Puyallup School District.
Metadata: A set of data that describes and gives information about other data.
De-Identified Data: Data that has all personally identifiable information removed.

Mandatory Security Requirements

Provider: Please look through the mandatory security requirements necessary for a partnership with the Puyallup School District. This section will require a signature from an authorized representative prior to acceptance.

The Puyallup School District requires all online service providers to meet the minimum guidelines established under FERPA, COPPA, HIPPA and PPRA. In addition, the district recognizes that all providers serve as "school officials" as outlined in FERPA. This entails:

- The school system retains direct control over all educational records and that the provider may not re-disclose educational records to any other person or party without authorization from the school system.
- The provider will not use any data to advertise or market to students or their parents.
- Providers will not change how data is collected, used, or shared in any way without advanced notice to, and consent from, the Puyallup School District.
- The provider will only collect necessary data to fulfill its obligations as defined in the agreement with the district.
- The provider is prohibited from selling data or metadata to any party.
- The provider is prohibited from mining data for any purposes other than those agreed to by the district.
- The district understands that providers will rely on one or more subcontractors to perform services. Providers shall agree to share the names of these subcontractors with the district upon request. All subcontractors and successor entities of the provider will be subject to the terms of this regulation.
- The provider will ensure that all data in its possession and in the possession of any subcontractors, or agents to which the provider may have transferred the data, are destroyed or transferred to the district

under the direction of the district when the data are no longer needed for their specified purpose, at the request of the district.

- The provider will not co-mingle data from other school systems or users with data from the Puyallup School District (per FERPA regulations).
- The provider will ensure that individuals employed by the provider may only access school records when necessary to provide the service to the Puyallup School District (per FERPA regulations).
- The provider agrees that all rights, including all intellectual property rights, shall remain the exclusive property of the district and that any provider has a limited, nonexclusive license solely for performing its obligations to the district. The district, including staff and students, will not grant providers or service any rights, implied or otherwise to data, content, or intellectual property except as expressly stated.
- Any data held by the provider will be made available to the district and/or parents upon request by the district.

The provider recognizes and agrees to the Puyallup School District's mandatory security requirements as outlined above.

Authorized Representative Signature: _____

Additional Security Information

Provider: Please review the following questions and provide a response.

Data Collection

- What personally identifiable data does the provider collect from users?

- What, if any, metadata is collected or generated by the provider, either directly or by third -parties (e.g., via cookies, plug-ins, ad networks, web beacons etc.)?

- What, if any geolocation data might be collected and how is this used?

- Does the provider de-identify data? If so, what is that data used for?

Network Operations Center Management and Security

- Does the provider perform regular penetration testing, vulnerability management, and intrusion prevention? If so, when was the date of the last test?

- 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 does the provider protect data in transit? (e.g., TLS, SFTP, HTTPS)
- If the cloud application is multi-tenant (several districts on one server/instance) hosting, how is data and access separated from other customers?
- Are physical server(s) in a secured, locked and monitored environment to prevent unauthorized entry and/or theft?
- Who has access to information stored or processed by the provider?
- 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?

Availability

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

Audits and Security Standards

- Does the provider offer the school system the ability to audit the security and privacy of its 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), and the Payment Card Industry Data Security Standards (PCI DSS) for specific types of data?

- Is your company SOC2 compliant? **If so, please attach a recent report.**

- Is the provider California Privacy Act (CCPA) compliant?

Data Breach, Incident Investigation and Response

- Describe the provider's breach plan including timelines and process for notification to the school.

- Will the provider inform or assist the school system with notifying the affected individuals in compliance with applicable laws?

- Will the provider assist the school system by providing a clear explanation of any such incident, including documentation on the root cause, scope, mitigation and steps taken to ensure protections in the future?

- Does the provider have an insurance policy around cybersecurity in place? If so, how will the district be compensated in the case of an incident?