Table of Contents

### Data collection

1. Is the use of the data considered a primary or secondary purpose that the data was originally collected for? Are those individuals supplying the data informed explicitly that the data will be provided for this reason and/or to this vendor?
2. What data is required for collection by the vendor? (refer SIF AU mappings)
3. Is any of the data collected by third parties (plugins, statistics, advertising, cookies etc.)?

### Data storage and access

1. Where is the information stored? Is the information stored in the same State/Territory as it was sourced/generated? Is it stored within Australia?
2. How is data protected “at rest”?
3. Is all or some data at rest encrypted (e.g. just passwords, passwords and sensitive data, all data)
4. What encryption method is used?
5. How will the information be stored? If the cloud application is multi-tenanted (several authorities’ data on one server/instance) hosting, how is data and access separated from other customers?
6. Are the physical server(s) in a secured, locked and monitored environment to prevent unauthorized entry and/or theft?
7. How is the data protected in transit? e.g. SSL, hashing? (SIF messaging generally use SSL/TLS)
8. Who has access to information stored or processed by the provider?
9. Is access logged?
10. Is access provided only to employees of the agency receiving the data or others?
11. When and how is access made available?
12. Are background checks or other vetting procedures performed on those with access (eg working with children checks)?
13. Does the provider subcontract any functions, such as analytics?
14. What is the provider’s process for authenticating callers and resetting access controls, as well as establishing and deleting accounts?

### Data and Metadata Retention

1. How does the provider assure the proper management and disposal of data?
2. How will the provider delete data?
3. Is data deleted on a specific schedule or only on termination of contract? Can the school/jurisdiction request that information be deleted? What is the protocol for such a request?
4. Can a copy of the information (including individual records) maintained by the provider be supplied at any time? How will this be provided?
5. Upon termination of contract/s, will the provider should return all records or data and properly delete any copies still in its possession?

### Development and Change Management Process

1. 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?
2. Are practices regularly audited?
3. 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?

### Audits and Standards

1. Does the provider allow for the audit of security and privacy of records by the jurisdiction/school?
2. Have the provider’s security operations been reviewed or audited by an outside group?
3. 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

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

### Data Breach, Incident Investigation and Response

1. What happens if the vendor experiences a data breach?
2. What are the vendor’s capabilities to perform security incident investigations or e-discovery? Are end user logs, administrative and maintenance activity monitored and are these logs available to the jurisdiction or school for incident investigation?