Questions to ask Third-Party Vendors

General Security

1. What security measures do you have in place to protect against common threats like malware, DDoS attacks, and data breaches?
2. Do you conduct regular security audits or penetration tests to identify vulnerabilities?
3. Are your systems and applications regularly patched and updated to address known security vulnerabilities?
4. What personal or sensitive data is currently stored? Please provide a list of fields captured, such as student photo, student name, bus route, scan time and date, and others. How long is the data retained?
5. How do you handle personal and sensitive information? How is it stored? How is internal access managed and monitored? Is data restricted to only those who need access to it?
6. What security requirements do you have in place to ensure the integrity of your system?
7. Do you have a web application firewall and how often?

Disaster Recovery

1. How do you detect, respond to, and mitigate security incidents or breaches?
2. Do you have a documented incident response plan, and how quickly do you notify customers in the event of a breach?
3. Have you experienced any security incidents in the past, and if so, how were they resolved?
4. What disaster recovery mechanisms are in place to ensure data availability and integrity?

a. Do you have a disaster recovery plan, and how often is it tested?

b. Do you have a business continuity plan, and how often is it tested?

5. How do you assess and manage the security risks associated with your third-party suppliers?
6. How do you ensure the security of your supply chain and prevent software supply chain attacks? If relevant, can you provide details on any subcontractors or sub-processors involved in delivering your services?
7. How frequently are backups of our data performed? What is the expected Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for data restoration? Are backups air-gapped or immutable?

Compliance and Certifications

1. What security and privacy standards or frameworks do you adhere to (e.g., ISO 27001 or any Edu specific certifications such as Safer Technology for Schools Safer Technologies 4 Schools – Supporting Schools, Teachers and Parents (st4s.edu.au)?
2. Have you undergone any third-party audits or assessments to validate your security controls?
3. Can you provide documentation or reports attesting to your compliance and security posture?

Vendor Risk Management

1. Do you have a vendor risk management program in place to assess and manage the security risks associated with any of your third-party suppliers, if applicable?
2. Can you provide details on any subcontractors or sub-processors involved in delivering your services?