MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

Education Report: Student Management System Vendor Market Options & Recommendations

To:	Hon Chris Hipkins, Minister of Education		
Date:	29 July 2021	**Priority:**	Medium
Security Level:	In Confidence	**METIS No:**	1266675
Drafter:	Neil Annenberg	**DDI:**	9(2)(a) [redacted]
Key Contact:	Wendy Hamilton	**DDI:** **Home (out of hours):**	
Messaging seen by Communications team:	No	**Round Robin:**	No

Purpose of Report

This report outlines options and makes recommendations for changes to the provision of school Student Management System (SMS) services that will create an uplift in capability, improve the integrity and security of student information. This is the second in a suite of papers providing advice on making school and kura ICT domains safe, including strengthening cybersecurity and protecting sensitive data in their systems:

1) Cybersecurity in schools and kura (submitted 25 June 2021, METIS 12262630)

2) Options to address challenges in the SMS market (this Education Report)

3) Te Rito and the deployment of the standardised Learning Support Register, due end August

4) Options to implement a framework to better support schools' IT, due at the end of September.

Summary

- In June 2021 we provided advice on cybersecurity in schools and kura in response to a rapid increase in cyber attacks. We identified two areas of particular concern; the foundational digital infrastructure in schools and kura, and the software they run that holds personal and/or sensitive data, such as student management systems (SMS) and learning management systems (LMS).

- In September 2021 we will provide you with advice on options to implement a comprehensive framework of IT support to schools and kura that would see a shift towards centrally managing critical IT infrastructure and services on behalf of schools and kura. The framework will take an end-to-end, whole of system approach to better support schools' digital environments.

- This paper provides a recommended approach to address the risks presented by school SMS services specifically. SMS are particularly vulnerable to attack given the sensitive nature of the information they hold and the highly variable cybersecurity maturity of vendors in the New Zealand SMS market.

- The risks are such that intervention is necessary, and requires significant change that will be complex to implement and take significant investment of time, resource and funding.

- Options considered a range from providing and mandating a single centrally managed school SMS through to requiring SMS vendors to meet functional, privacy and security standards as a condition of being contracted to provide SMS services.

- Our recommendation is for a 'managed choice' solution whereby the Ministry procures, funds and manages 3rd party SMS services that meet the required capability and quality uplift, on behalf of schools. This option strikes a balance between replacing an unregulated market with the Ministry as single supplier, whilst providing the desired measures and protections for the security and integrity of core school systems and student information.

- At this stage we have not had sufficent time to provide an estimate of the development and deployment benefits, costs, effort, risks and considerations for a richer comparison of the available options. We propose that these will be articulated within a strategic business case, providing the necessary basis for a budget bid. We note that in addition to one-off costs, we expect the overall ongoing cost of providing student management services will increase, largely because the uplift in service expectation, capability and information security sets a much higher bar compared to today's market model, typified by low margins and regarded by schools as a fiscal overhead.

Recommended Actions

The Ministry of Education recommends you:

a. **agree** that the managed choice solution is the most appropriate approach to deliver the required capability, quality and security uplift for school SMS services.

Agree / Disagree

b. **agree** that we will outline the options, benefits, cost estimates, implementation, change management and service delivery implications of a managed choice solution for school SMS services, as part of a broader strategic business case and Budget 22 bid to implement a comprehensive framework for ensuring schools' IT systems are safe, secure and fit for purpose.

Agree / Disagree

c. **agree** to further discussion about the managed choice solution, to ensure alignment of expectations in the short, medium and long term, and associated implications. This includes using the school SMS vendor market as an early example of the broader framework to better support schools' IT as part of our Digital Strategy.

Agree / Disagree

d. **note** the current school SMS service delivery environment does not meet government or the sector's needs and expectations for the integrity and security of student information.

Noted

e. **note** that to ensure trust and confidence in the education sector's increasing levels of data interoperability, access, and sharing, we need to create an uplift in accountability, cohesion, awareness, and capability in the security and privacy of student data.

Noted

f. **note** the Ministry's work to date, including the Te Rito programme, to mitigate the overall risk profile and improve confidence in the secure use and flow of student information.

Noted

g. **note** that any change in the school SMS service delivery environment will establish precedents and have implications for the wider digital infrastructure and software used by schools and kura, including Learning Management Systems, and beyond the schooling sector into early learning and potentially tertiary systems.

Noted

h. **note** that the Ministry proposes to establish a limited panel of accredited school SMS providers and certified products, ensuring an uplift in capability, security and integrity but reducing choice for schools and kura.

Noted

i. **note** that the Ministry proposes to take accountability for and manage the governance, commercial, funding and relationships with school SMS providers on behalf of schools and kura.

Noted

j. **note** that the recommendations in this paper are subject to further analysis and socialisation across the sector, so that we can elaborate on the approach, implications and likely timeframes.

Noted

k. **agree** that this briefing is not published at this time under the provisions of section 9 of the Official Information Act: Free and Frank advice, section 9(2)(g)(i) and commercial sensitivity in relation to IT providers 9(2)(b)(ii).

Agree **Disagree**

Alexander Brunt
Deputy Secretary
Evidence, Data, and Knowledge

29/7/2021

Hon Chris Hipkins
Minister of Education

27/ 8/ 2021

Introduction

1. On 2 June 2021 you requested a briefing on school SMS vendor market options and recommendations, following a strategy meeting to discuss the Te Rito programme and broader issues raised about cybersecurity vulnerabilities. You asked that we consider the sourcing environment and associated impacts on the school SMS market.

2. On 25 June 2021 we provided advice on strengthening cybersecurity in schools and kura, which described the elements of a school's digital environment that are particularly vulnerable to cyber-attacks, privacy breaches and/or operational failure. We noted two areas of particular concern: schools' foundational IT infrastructure and the software schools use that hold sensitive data, such as SMS. We advised that many schools lack the capacity and capability to manage and adequately protect their IT systems, and that intervention to provide better support is urgently needed.

3. This briefing note is one of four reports on options for strengthening schools' IT systems, and subject to your agreement to a framework set out in d) below, will be followed by a strategic business case and Budget 22 bid to implement a comprehensive framework for ensuring schools' IT systems are safe, secure and fit for purpose:
   a. Initial Advice on Cybersecurity in Schools and Kura, dated 25 June 2021 (METIS 1262630);
   b. SMS Vendor Market Options and Recommendations (this paper);
   c. Standardised Learning Support Register and Te Rito National Deployment Options, due at the end of August;
   d. Options to implement a framework to better support schools' IT, due at the end of September.

Background and context

4. Schools and kura are largely responsible for procuring and managing their own IT, including being accountable for contracting providers of digital applications that hold identifiable student-level data, such as SMS, LMS, pastoral care applications, and generic commercial applications like Xero.

5. School boards are legally obligated to protect personal information, but school systems do not sufficiently support them in this regard. Nor are boards or principals experts in contract management and the details of regulatory controls. While the Ministry provides guidance, clarification and support across a range of topics, the current commercial and accountability model for 3rd party systems suppliers to schools limits the Ministry's mandate to an influencing role.

6. The exception to this is where the Ministry centrally procures and funds access to the Google and Microsoft suites of applications for schools and kura to select from.

7. Given the rapidly escalating risks of cyberattacks and data breaches, it is no longer tenable for individual schools to procure, maintain and assure the provision of core ICT infrastructure services and functions, especially those that manage sensitive student information.

8. In February 2020 we briefed you on the Te Rito programme (METIS 1214953 refers), which has surfaced security and privacy risks in the school SMS vendor market. These risks largely relate to network and data security architecture, access management control systems and processes, and tracking and logging systems. Systems that are hosted on school premises are subject to additional risks, as school staff are responsible for management controls and system updates.

9. These risks are not new, and Te Rito will improve the security and integrity of student information flow between school systems and provide a central repository (back-up) of student information.

10. Te Rito has progressed its work to mitigate these risks, but there is more to do. Work to date includes establishing and publishing an internationally recognised technology and data specification that lays out the data standards that SMS providers integrating with Te Rito must meet. Te Rito's security and privacy standards are consistent with New Zealand government standards and legal obligations for any entity working with sensitive personal information.

11. Te Rito has also commenced an in-depth security and privacy discovery exercise, to assess if school SMS provider systems meet government standards and, if not, identify what remedies might be necessary. The discovery exercise was developed in close collaboration with a similar process undertaken by Australia's Safer Technologies 4 Schools initiative. Our discovery exercise is due to complete in December 2021.

12. The Ministry's 'first principles' approach to information flows between school systems means that safeguarding information is an integral part of protecting students from harm. Student information is treated as taonga, and protecting the integrity and security of student and ākonga data is a critical priority.

13. 9(2)(b)(ii) [redacted]

14. Covid-19 also highlighted existing inequities and increasing reliance on access and use of data across the sector. Initial post-Covid lockdown discussions with other sector agencies in mid-2020 indicated broad support for a coordinated approach to an uplift in 3rd party vendor security and privacy capability across the sector. There is appetite for change.

Our requirements of Student Management Systems

15. There are currently hundreds of providers of systems and applications in the education sector, including on-line subscription applications (e.g. parent portals), bespoke systems provided by small-medium companies (e.g. school SMS), and commonly utilised applications provided by large international ICT service providers. Many parent and student portals or apps have some degree of integration or data sharing with SMSs, creating additional layers of technical complexity and security risk.

16. Our digital strategy provides the framework within which the functions, and information flows, enable an education system that learns. For example, in the future Te Rito will provide the common platform that integrates the core SMS information flows and enables streamlined processes for e.g. enrolment and roll returns. We are also contributing to the Digital Identity Trust Framework being led by DIA, including potential use cases to support parent and student portals to securely access their information.

17. Our early assessment of market options and role of the Ministry is in context of schools' and the Ministry's needs and expectations of SMSs, including how these school administration systems fit within the broader digital ecosystem. There is no standard or commonly agreed definition of an SMS, but Appendix 1 outlines the Ministry's perspective of the SMS Eco-system, which shows the few core SMS features provided by all providers, a fuller list of features provided to varying degrees by SMS providers, and related features provided by other school systems. There is a high degree of variation in how schools and kura acquire these features. The narrow range of core SMS services, functions and features:
    a. are the education provider's system of record for core student management processes and data;
    b. enable and support required Government reporting and data collection;
    c. are able to exchange core student data with other systems, supporting school processes and data flows.

18. Within this, the core information they contain and processes they support are:
    a. student identity and demographics;
    b. caregiver details, progress reports, and pastoral care;
    c. enrolment, teaching groups, and attendance.

19. This narrow range of core functions and information is typically expanded to varying degrees by SMS providers, providing schools with additional value and utility (sometimes at extra cost), that would otherwise need to be provided by other systems, creating another layer of integration complexity. These additional SMS features contribute to the school's selection of a particular product, and include things like complex timetabling for secondary schools, recording progress and achievement, behaviour records, managing fees and donations, integration with learning platforms or apps, and local analytics. It is difficult for any a single system to encompass the whole range of functions and features that meet the needs of all education providers, and ultimately form part of a rich virtual learning environment.

20. With that in mind, the core SMS fulfils a distinct and specific purpose within the broader education provider and digital ecosystems, but over time has grown organically to provide additional, but necessary, features and information flows. These in turn sit alongside and need to integrate with systems that support curriculum progress, educational achievement, learning management, learning support, pastoral care, student and parent participation.

Alternative governance, commercial and relationship models

21. Education sector agencies (from early learning through compulsory to tertiary) typically have a low level of governance and oversight across the market entry of these systems, their features, the commercial arrangements with education providers, and the operational, technical, security and privacy standards. Direct arrangements between sector agencies and SMS vendors do exist in some cases, but typically cover the technical operation of agency interfaces and/or data accuracy, not verification of data security and privacy controls.

22. To address the underlying risks associated with this market dynamic, we need to achieve a capability uplift that creates higher levels of trust and confidence in the security and privacy of student data across the ecosystem. We also need to normalise our shared understanding of what features are provided by which systems, and by whom. This requires market intervention above and beyond increased levels of engagement, awareness and support between agencies, boards of trustees, principals, students, whānau and vendors. Specifically, we recommend changes to the capability and scope of the SMS market, and to the commercial, funding and relationship model.

23. To assess the pros and cons of available options, we have articulated the range of market options on a continuum of intervention across inter-related digital environments. This covers the main options for governance and assurance, commercial and relationship management, sector education and support. See Appendix 2: Continuum of SMS vendor commercial and relationship model options. The options are inter-related. For example, if the Ministry were sole supplier of the SMS, vendor contract management would not be required, but service management agreements with schools would be.

24. The pros, cons and variables of the most likely options are summarised in Appendix 3, SMS market service provision - pros and cons, including comparing a Ministry provided SMS service to a curated and managed vendor panel.

25. A Ministry provided SMS removes risks related to 3rd party vendor dynamics by transferring the roles and responsibilities to the centre. This in turn requires the centre to build and manage the necessary services, functions and capabilities. The risks of ongoing provision of a centrally provided solution service are largely about the reduction in market and system resilience and innovation. From an implementation perspective, it introduces design, build, change management and transition risks and costs compared to leveraging existing functions and operating models provided by the market.

26. Given the wide range of functions and features required by schools, our first consideration is whether to constrain a centrally provided service to the narrow range of core functions, focussing on core capability and information flows, reducing complexity, but leaving gaps. Essentially a 'skinny' SMS, supplemented by other services.

27. A centrally provided 'skinny' SMS solution is attractive in so far it constrains scope and simplifies operational consistency that can be managed from the centre. As a new function, it will require solution design, development and deployment, new policies, frameworks and support structures, including service delivery to schools.

28. Any broader service features omitted from the 'skinny' core will still need to be met elsewhere (or else cause degradation of service and frustration), creating different

system integration risks and requiring additional controls to ensure security of information flows between core and additional services.

29. A single centrally provided 'full scope' SMS that meets the vast majority of all education providers' needs would remove the integration risks with non-core SMS. However, by extending the functional scope beyond the 'skinny' core it materially increases the design, build, implementation and transition risks and costs to the Ministry. It also increases the data migration effort between school systems. This would require a large scale implementation programme, carrying very high implementation and change management risk.

30. Importantly, with a likely design, build and implementation timeframe of several years for even the 'skinny' SMS, we would still need to drive an overall cybersecurity and capability uplift in the meantime. Mobilising and incentivising any uplift from the current 3rd party providers faced with loss of their business, is complex and carries its own risk profile. This would require additional support, new governance levers and mitigation strategies to protect ongoing services to schools and to enhance the protections around student information. In other words, we still need to drive the 3rd party providers towards a higher quality standard.

31. We are therefore seeking a balance of functional scope, secure data flows and efficient service delivery with cost, risk and complexity to deliver and maintain, whilst providing foundational accreditation and assurance.

Our recommended approach – managed choice

32. Our Education Report dated 25 June 2021 'Initial Advice on Cybersecurity in Schools and Kura' (METIS 1262630) proposed that SMS, LMS and other higher risk systems containing student data would in future be provided under a 'Managed Choice' scheme, with schools able to select from a limited set of centrally procured and/or centrally funded options. This approach could include resetting the contractual arrangements for education software, with the Ministry procuring vendors directly on behalf of schools. See Appendix 4: A possible framework for supporting schools' IT.

33. Our recommendation is for a limited panel of accredited[1] 3rd party vendors, centrally procured, managed and funded to government standards of contracting, service provision, and security. Accreditation provides quality assurance, whilst Ministry procurement and contract management removes the administrative burden on schools. This approach also allows for functional flexibility that specialist providers have already developed to remain competitive. This option aligns with the existing integration approach to Te Rito – providing additional resilience and assurance, e.g. a back-up of SMS data. By leveraging the best of the existing vendor capabilities, we reduce the overall cost and risk to implement, and limit the impact on private sector employers. To a large extent, this approach accelerates the anticipated market disruption that Te Rito was likely to trigger.

[1] The extent of accreditation and assurance will be explored in further detail at a later stage, as there are a range of options with varying degrees of intensity, functional coverage and cost/benefit.

34. The current development of an SMS catalogue to facilitate the transition from Assembly is providing valuable insights into vendor functions, capabilities and characteristics. This includes functions and features, licence fees, service management, and willingness to engage. This information, combined with Te Rito's security and privacy assessment, will inform a fuller assessment of the market's capability and responsiveness to meet our long term expectations, and provides a head-start for the creation of a panel.

35. As the central contracting, funding and accrediting party, the Ministry obtains the necessary direct levers for control, the absence of which has to date exposed the sector security risks, frustrated our progress and complicated our ability to assert authority. This approach leaves space for further evolution of the market, so we can adapt as we implement the refreshed Digital Strategy, progressively improve cybersecurity, and assess the market response. In essence, we reserve the right to extend our reach.

36. Fewer providers and removal of direct control for schools will be outweighed by an uplift in quality, the reduced funding management and administrative burden, and confidence in information security. Many schools already believe that the Ministry accredits SMS vendors, and we believe that formalising the quality standards and reducing the burden will incentivise schools to use the SMS panel.

37. The table below summarises key aspects of the Managed Choice option we recommend as the preferred option, the implementation of which is subject to more detailed analysis and pending your agreement.

Preferred Option: Managed Choice	**Rationale**
Ministry as contracting and funding party (government agency procurement & contract management framework)	• Removes the burden on school/board of trustees • Provides Ministry leverage and influence • Leverages Ministry core capabilities • Ensures standardisation of T&Cs • Provides transparent cost/value indicators and control mechanisms
School SMS vendor panel (pre-qualified vendors from which schools can choose)	• Provides for product and service specialisation within an agreed core set of functions, features & services • Promotes competition, innovation and new entrants • Avoids single-supplier risk • Leverages commercial market capabilities • Avoids additional Ministry burden as sole supplier • A proportion of schools will not need to change providers • Maintains market and system resilience
School SMS product certification & vendor accreditation (independent verification of government standards, capabilities, services and controls)	• Quality assurance • Binds product and vendor as a single supply chain • Constrains sub-contracting/3rd party arrangements that create point of failure risk • Promotes compliance with government & industry standards • Providers can evidence credentials to overseas markets

Ministry standards authority across SMS vendor market (oversight of ongoing service delivery and adherence to standards)	• Oversight and monitoring to agreed rules, behaviours and tolerances • Leverages existing Ministry powers • Avoids legislative change • Consistent with similar agencies, e.g. health
Ministry hosted test environment & tools for SMS systems	• Ensures technical consistency & data integrity • Visibility of technical capability (pass/fail) • Avoids duplication in the market • Enables technical alignment with other systems, e.g. Te Rito, ELI
Charters, codes of practice, polices, processes & frameworks for school SMS systems and services	• Practical & accessible application of service & quality standards • Standardises & supports school/vendor operating models and processes • Assists schools to manage day-to-day service delivery and good security practices

38. Whilst no system infrastructure is 100% safe, the Ministry-led, market-enabled model will create the most appropriate controls, protections and assurances for the provision of school SMS services to schools, to protect the security and integrity of student information whilst maintaining market and system resilience.

39. Implementing a Managed Choice approach requires a significant amount of work:
    a. for schools, there will be operational disruption for those transferring to alternative service(s), changes to accountabilities, and involvement in Ministry-enabled uplift of privacy and security capabilities.
    b. for vendors, we will need to support them to understand and meet their security and privacy obligations;
    c. for the Ministry, we will need to develop new systems, policies, frameworks and support structures, requiring a significant internal programme, and leading the sector though a considerable period of change to their current service delivery, roles, capabilities and accountabilities. We will work with other agencies, e.g. GCDO and Ministry of Health, to ensure all of government alignment and to learn from similar examples.

40. We will provide further information and additional levels of detail at the end of September in our presentation of options to implement a framework to better support schools' IT.

41. We will include the implementation of a managed choice solution for school SMS services as part of a broader strategic business case and Budget 22 bid to implement a comprehensive framework for ensuring schools' IT systems are safe, secure and fit for purpose. It will outline the case for change and analyse the various solution options against agreed outcomes and success criteria. The business case will also identify the high-level implementation approach, conditions for success, risks, benefits and costs, our commercial approach to managing the 3rd party provider market, and our management approach to support ongoing service delivery to schools. It will include a high-level timetable and transition options, e.g. novating current school SMS vendor contracts to mitigate the impact of market exit.

What this means – conditions for success

42. Given that safeguarding information is an integral part of protecting students from harm, and we treat student information as taonga, any Ministry intervention in the current SMS market dynamics needs to establish conditions for success and satisfy a number of elements, including:
    a. the key capabilities required of 3rd party vendors to support the Education System Digital Strategy2. This includes product functionality, service reliability, financial stability and operational competence.
    b. our vision for the commercial and relationship model(s) across the education sector. This includes our sourcing strategy, the competitive environment we require, the commercial and technical standards we expect of the private sector.
    c. the target operating model and accountability framework between sector agencies and 3rd party vendors across the sector. This includes roles and responsibilities to govern, manage, assure and improve data interoperability standards and capabilities.
    d. the regulations, standards, frameworks and policies that we want to establish across various parts of the data ecosystem. This includes what behaviours we require and expect of those participating in it.

43. We also need to consider our appetite for (and pace of) change, including scale of market disruption, in context of the gap between desired and actual level of security and privacy capability, confidence and assurance across the system, schools' readiness for operational disruption.

Implications and considerations

44. The creation of an accredited SMS vendor panel and associated control mechanisms would sit within a broader shift in the operational, commercial, and ICT landscape for other school systems.

45. From an operational perspective, our priority is to minimise administration overhead whilst creating the necessary uplift in the security of student information. Schools will value the reduced burden of systems administration, providing there is minimal disruption to their operational processes, e.g. financial management and reporting, supported by SMS systems. SMS are part of an integrated and complex workflow, and whilst the fundamental needs are similar for all schools, how these are applied and prioritised varies widely. For example, SMS systems have core common features and services, e.g. the student record, but are selected based on discretionary features and functionality such as usability, integration with other systems and parent/student apps, reporting, and data analysis. One system in particular, 9(2)(b)(ii) supplies 9(2)(b)(ii) of the secondary school market, in large part because of its sophisticated timetabling functionality and responsiveness to school requests for new features. This lends itself to a managed choice, rather than a one-size-fits-all approach.

---

[2] Within this, our draft Digital Eco-system for Learning provides a future-state map of education sector systems and functions, including SMS in relation to the virtual learning environment.
[3] As at 1 March 2021

46. ICT functionality and controls are part of the approach to reduce cybersecurity risk. Of equal importance is awareness, capability and capacity of school staff and anyone else in the information flow to apply robust security and privacy practices. Human error is a significant factor in breaches, especially where systems, processes and data are heavily integrated and widely distributed. An uplift in training and awareness is key, as is 'security by design', and the ability to monitor, prevent and respond to potential and real risk events. Any approach we take to market intervention will require significant investment in school capability, plus our collective ability to detect, prevent and respond to risks. We would also leverage existing providers, e.g. Network 4 Learning, where appropriate.

47. From a transitional perspective for schools, minimising disruption, maintaining data integrity, and ensuring service continuity are critical for success. Our current experience with the Assembly transition is instructive, and demonstrates the significant effort required of the Ministry to support any transition between providers (or to a single provider). The proposed product certification approach also provides an opportunity to clarify the product features provided, and enables a high degree of data standardisation, which aligns to the approach already undertaken by Te Rito and the standardised Learning Support Register. The migration path to accredited vendors and certified products will need to balance the operational disruption and service continuity, with urgency for an uplift in security. We will need to implement this in stages of increasing maturity.

48. The transitional process for the vendor market is of particular concern for any new market model. Current school SMS vendors will variously perceive this as an opportunity or a threat and will either grasp the opportunity to upgrade their capability, or retreat from the market if the cost and/or time to bridge the gap is too high. Potential new entrants will also emerge. Vendors choosing not to remain, or failing to meet the new standards, may not exit in a managed way, exposing continuity of supply risks and access to student data – 9(2)(b)(ii)

49. Downstream implications of vendor market disruption include positive and negative economic and employment impacts for SMS vendors, which are mostly small to medium companies.

50. The Ministry's market intervention plan will need to provision for the cost and effort required for vendor systems to be assessed against the new standards and implement any changes. This will require a different approach than a previous attempt to accredit vendors, justified by a stronger rationale and heightened expectations. Ministry support will pay dividends as the review process generates increasing levels of maturity and sends signals to other parts of the sector.

51. The proposed approach does not preclude a school choosing to utilise a provider that is not on the Ministry's panel, by severely limited exception, in order to satisfy unique circumstances, e.g. an extreme risk of denial of service. We would still require the vendor to meet the security, privacy and data integrity standards, and be subject to some degree of ongoing checks and balances, at their cost. Material implications of this flexibility relate to Ministry influence and end-to-end cohesion of the system, specifically:
    a. by the school retaining the right to select and contract directly with their chosen provider, the Ministry forgoes influence because there is no direct commercial relationship, but yet must be able to assert and seek ongoing assurance of data integrity and security standards.

b. the Ministry would need to establish mechanisms, e.g. explicit agreement with the school, to assert certain conditions unrelated to security and privacy, e.g. automated reporting of roll return and attendance data, and connectivity to Te Rito.

52. We suggest that non-panel membership would be by severely limited exception and subject to a very high 'bar' for approval. Otherwise the impact on competitive advantage of panel membership and lost influence over vendors will erode broader value for the Ministry and sector cohesion, especially as the ICT and data infrastructures evolve, and student data becomes more readily accessible and transferable across the system.

53. In anticipation that a significant vendor with a unique product feature may choose not to join the Ministry panel and/or fails to meet the accreditation standards, we propose to develop a range of progressive steps to encourage, assist or require compliance. At one end of the continuum, we aim to mitigate the risk of certain functionality, e.g. complex timetabling, being lost due to mass market exit of certain provider(s). This may require a targeted intervention to protect ongoing provision of service whilst alternate providers are identified, or specific solutions are developed, e.g. a timetabling app for all vendors/schools to integrate with. The Ministry's procurement, commercial and technical provisions for a range of vendor responses will be further explored in the strategic business case.

54. Pending confirmation of the detailed approach, Te Rito offers an opportunity to create a 'landing stage' at which vendors' secure integration with Te Rito is a milestone event on the journey towards security and privacy standards being met. It introduces substantial security and privacy controls regarding information flow, and builds the Ministry's repository (back-up) of information held in SMSs.

55. By establishing the standards for product certification and vendor accreditation, and assessing the gap for current vendors, we will likely evidence material concerns about existing cybersecurity or other risks. At any stage during the transitional process, we may need to alter our approach to specific current vendor services. The security and privacy risk assessment being undertaken by Te Rito will inform this, noting that it is focussed on technical and operational risks relating to SMS integration with Te Rito, and excludes things like SMS integration with other school systems or 3rd party apps.

56. From a technical perspective, bridging the gap for school SMS vendors is part of the wider and matrixed data ecosystem. Other 'weak links' will need to be addressed progressively, so that we remediate and mitigate the overall risk profile. Hence the approach to school SMS vendor systems outlined in this paper is a precursor to broader systemic change requiring a sustained and concerted strategic shift in technology and capability across the sector. We will provide further advice on the broader approach and implications for the schools' ICT infrastructure as a whole, at the end of September.

57. From a governance and relationship perspective, we propose to establish, publish and implement agreed standards and expectations, at both technical and operational levels. Many of these standards and good practice models already exist across government, but may need to be adapted to meet our needs.

58. From a data governance perspective, the rights of iwi Māori to have decision rights over the collection, use and management of Māori data as taonga is a growing call to action for government departments to give effect to Te Tiriti o Waitangi in respect to Māori data. Rights and expectations regarding data governance will inform our requirements of the SMS market. This includes consistent provisions for data storage, sharing, access and use.

59. Similarly, we will also develop an assessment, measurement and monitoring framework for schools and the vendor community, to ensure currency, consistency, and responsiveness to gaps as they arise. This includes an agreed governance framework and decision rights to oversee the effectiveness of a centrally managed but operationally distributed model and, if necessary, apply interventions. This regime also ensures the provision of ongoing support and continuous improvement regarding good practice. A Ministry provided SMS solution would also require service delivery assessment, measurement and monitoring, albeit from a different perspective.

60. The Ministry will work with school boards, unions, and peak bodies such as NZSTA to clarify implications and develop an action plan for changes to governance accountabilities, and the support structures for schools. Our proposed approach to ICT accountabilities and operational management has parallels with current changes to property management in schools.

61. A centrally procured and accredited 'Managed Choice' model will include centralised contract management, with implications for how the services are costed, funded and administered. For example, subject to further exploration of policy and regulatory implications, we propose that services will be funded directly by the Ministry, rather than via the Ops Grant, which would remove another aspect of school administration, and empower the Ministry to oversee the derived value to agreed quality standards and cost.

Next steps

62. The Ministry will continue to develop its approach to the broader framework to better support schools' IT, reporting back to you on this and options to recommence the deployment of Te Rito and the standardised Learning Support Register.

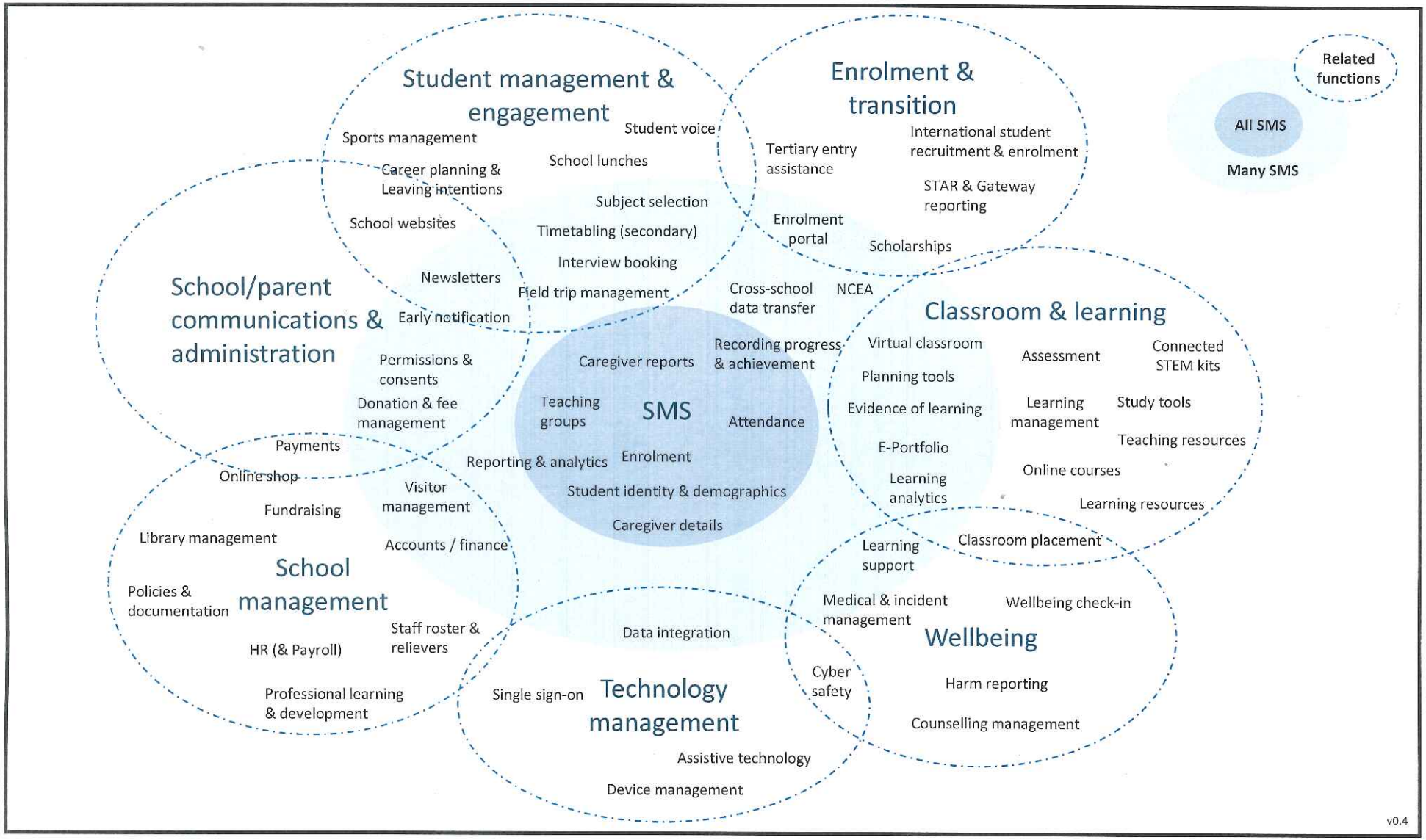
63. The Ministry will undertake analysis of policy and regulatory implications and options for:
    a. changes to the respective roles and responsibilities of the Ministry, Boards of Trustees, schools, and 3rd party vendors;
    b. changes to the current funding mechanisms and processes;
    c. applying existing and enacting new mechanisms to determine, measure, and assure compliance to the new standards, including sanctions for non-performance.

64. Pending your agreement, the Ministry will include the implementation of a managed choice solution for school SMS services as part of a broader strategic business case and Budget 22 bid to implement a comprehensive framework for ensuring schools' IT systems are safe, secure and fit for purpose. This will outline the case for change and analyse the various solution options against agreed outcomes and success criteria.

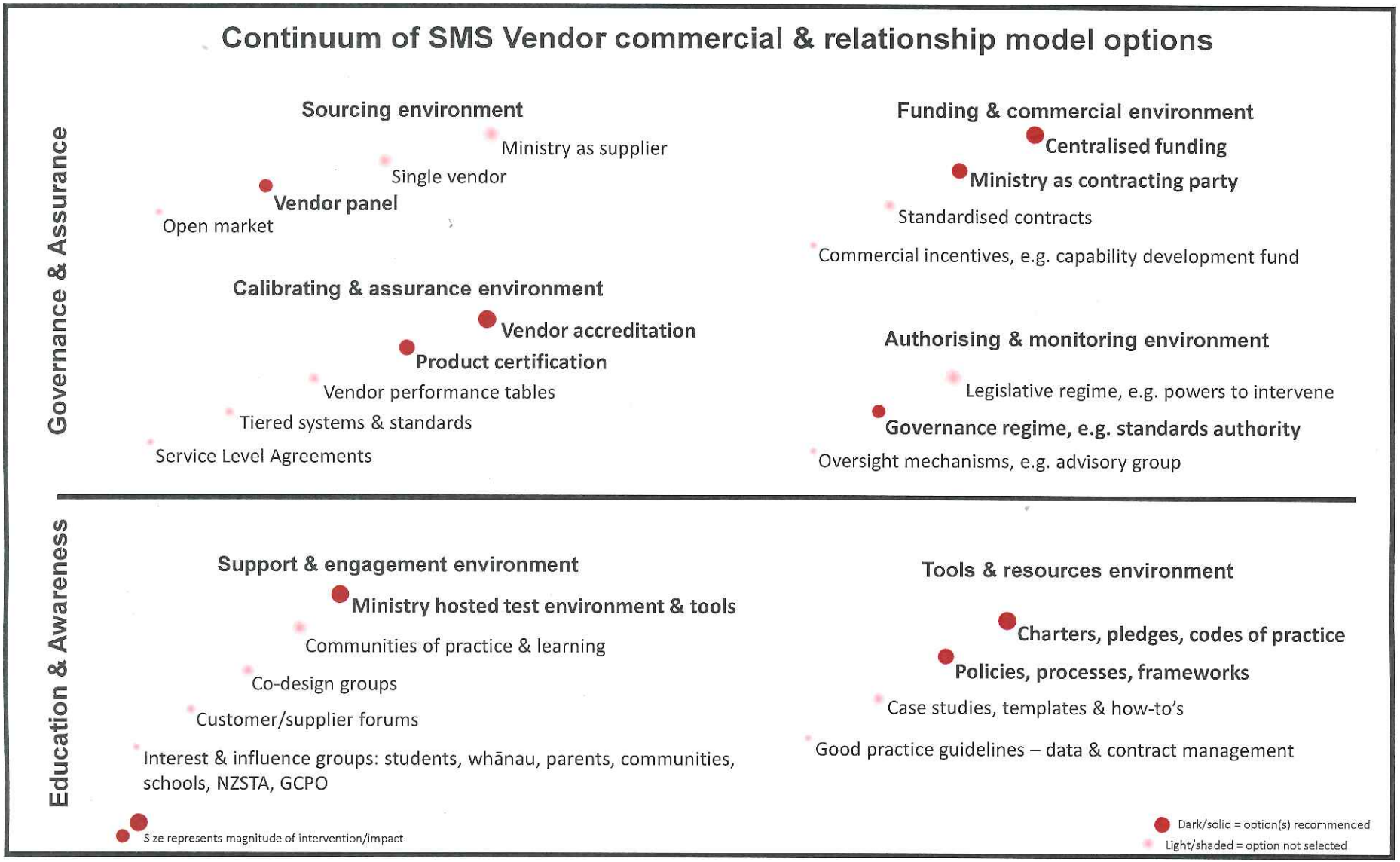
65. Pending your agreement, the Ministry will facilitate a strategy session with responsible Ministers to discuss the options and recommendations in this paper, with a focus on the implications of remediating the security of student information in school SMS vendor systems in the short, medium and long term.

66. Pending your agreement, the Ministry will work with other Education sector agencies, lead all-of-government agencies (e.g. Te Kōtui Whitiwhiti - Digital Public Service branch) and agencies with experience in similar scenarios to ensure alignment.

Appendix 1: Ministry perspective of the SMS Eco-system



Appendix 2: Continuum of SMS vendor market commercial and relationship model options



Appendix 3: SMS market service provision - pros and cons

Option	Pros	Cons	Risks & Variables
Ministry SMS service (centrally provided)	• Full consistency across the school network • Full economy of scale • Direct responsibility for service features and functions • Ministry controlled security and privacy • Centrally managed data integration • No management of vendor or product performance	• Single point of market and system failure • Longest timeframe to implement • Highest design & build effort • Highest data migration risk • Ministry resource intensive • Full range of schools' needs unmet • Restricts innovation • No competition	• Still requires uplift of SMS provider and school/kura capability whilst Ministry service is developed • Ministry bears sole risk of design, build and operation • Extends Ministry capability as service provider to schools, requiring 'internal' service standards
Ministry-contracted SMS vendor panel (managed choice)	• Core functional consistency across the school network • Relative economy of scale • Flexibility of service, features and functions, within boundaries • Ministry assured security and privacy • Promotes innovation & competition • Ministry leverage via direct vendor contracts and relationships, e.g .Te Rito integration • Maintains market and system resilience	• Ministry has burden of contract and relationship oversight • Maintenance of certification & accreditation standards	• Vendor non-performance falls to Ministry • Cost of certification & accreditation standards can be shared with vendors • Networked data integration with central systems • Provides can evidence credentials to overseas markets • Ministry asserts required service features and functions
School-contracted SMS vendor panel (managed choice)	• Core functional consistency across the school network • Flexibility of service, features and functions, within boundaries • Ministry assured security and privacy • High level of data integration with other Ministry systems • Promotes innovation & competition	• Schools retain burden of contract & relationship management • Ministry has less leverage over vendor relationship, e.g. for Te Rito integration • No economy of scale for contract management	• Vendor non-performance falls to schools (but in reality, major issues pass to Ministry) • Requires contract & service standards to be locally managed

Appendix 4: A possible framework for supporting schools' IT (Draft – not government policy)

Centrally provided

Centrally-funded & managed core services

For example:
Office suites (Microsoft & Google)
School enrolment portal
HR management
Cyber safety & security, identity management
Managed devices for staff & students
Campus infrastructure
Internet services (N4L)

Rationale
- Necessary for system security, coherence and equity for foundational services
- Economies of scale reduces cost
- Most opportunity to influence service design
- Promotes efficient administration of the education system
- Enables a student-centred system

Implications
- Least local choice, localisation, innovation
- More implementation effort in the centre (less overall for the system)

Managed choice

Centrally-procured higher risk & commonly used services

For example:
Student Management Systems (SMS)
Learning Management (LMS)
Learning analytics
Parent communications
Pastoral care & behaviour mgmt.
Building systems (CCTV, security, meeting room technology)

Rationale
- More hands-on approach for higher risk services
- Cost savings through centrally negotiated contracts for commonly used services
- Reduces procurement and onboarding effort for schools
- Greater opportunity for Ministry to drive system-level outcomes
- Preserves a degree of local choice

Implications
- Less local choice, localisation, innovation for core services
- Moderate implementation effort in the centre

Local choice

Wide range of lower risk, localised services

For example:
Learning tools and resources
Courseware
Content creation
Finance management

Rationale
- Providers have flexibility to use tools that suit their local needs
- Catalogue provides transparency around level of risk for each service
- Allows flexibility in level of assurance
- More manageable approach for the large number of tools in use.
- Minimises impact on market innovation

Implications
- Minimum standard will be required to be listed on catalogue
- Standardisation has potential to increase innovation
- Least intrusive, and lower (central) implementation effort
- More risk & effort left with schools

Devolved (current)

Full local choice, most services sourced by individual schools

For example:
Student Management Systems (SMS)
Learning Management (LMS)
Learning analytics
Parent communications
Pastoral care & behaviour
Building systems
Campus infrastructure
Most cyber security
Most identity management

Description
- Some infrastructure managed centrally on opt-in basis (e.g. N4L)
- Some services licensed centrally but configured & managed by schools (e.g. Microsoft, Google)
- Most services procured and managed individually by schools
- Limited, generic guidance provided centrally
- Limited support provided centrally
- No catalogue of accredited services

Implications
- Most local choice, however innovation constrained due to lack of standardisation
- Most risk & effort left with schools
- Significant, system-wide cyber-security uplift not feasible
- Difficult to deliver student-centric services
- Poor value for money at system level

Accreditation & assurance (foundational)
- Ensures digital services meet privacy, security and interoperability standards, and that residual risks are understood
- Supports schools in meeting their privacy and security accountabilities
- Supports data portability and integration with common platforms to support seamless education delivery
- Alignment with international standards (particularly AU) supports local vendors to grow export opportunities