MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

Education Report: Strengthening cybersecurity and IT support in kura & schools

To:	Hon Chris Hipkins, Minister of Education		
Date:	8 October 2021	**Priority:**	Medium
Security Level:	In Confidence	**METIS No:**	1269453
Drafter:	Margaret-Anne Barnett	**DDI:**	9(2)(a)
Key Contact:	Stuart Wakefield	**DDI:**	
Messaging seen by Communications team:	No	**Round Robin:**	No

Purpose of Report

This report seeks your input on a proposed approach to strengthen cybersecurity and IT support to the compulsory schools' sector and is one of several papers we have provided recently on mitigating the risks of escalating cyber-attacks and privacy breaches across the education system.

While cybersecurity is a critical driver, this paper also addresses the broader need to support kura and schools' IT as digital technologies get more complex to manage and schools are increasingly dependent on their IT systems to operate effectively.

Summary

- This paper expands on advice we provided on 25 June 2021 on cybersecurity in kura and schools, and on 29 July on the SMS vendor market, following which you agreed to the Ministry providing further advice on better supporting schools' IT.
- We propose a shift to centrally managing critical digital services on behalf of kura and schools, addressing two areas of concern as a matter of urgency; the core digital infrastructure necessary to keep kura and schools operating, and the applications they run that hold sensitive data, particularly SMS. As noted in previous advice, we are implementing tactical measures to improve cybersecurity but these will not alleviate the burdensome demand on boards to procure and manage their own IT systems, which is the broader focus of this paper.
- Following advice on SMS on 29 July 2021 you agreed that a 'managed choice' solution is the most appropriate approach to deliver the required capability, quality and security uplift for school SMS services. This paper provides advice on next steps, starting with establishing an assurance framework to establish appropriate IT standards for SMS and other systems and applications used by schools against appropriate IT standards.

- These proposals will require changes in policy settings, including reviewing the way schools are funded for IT and the roles and responsibilites of the Ministry, boards of trustees and IT providers. This may include mandating the use of assured technologies that handle personal data such as SMS, or applying conditions that schools kura and schools must meet if they opt-out. We also recommend mandatory reporting of cybersecurity incidents and privacy breaches. Any such changes will have commercial implications for IT providers, some of whom could struggle to meet the standards required to continue to operate in the education IT market.

- Change at this scale will take time and investment, and a significant uplift in digital capability across the sector. We estimate requiring funding of up to 9(2)(f)(iv) over four years (more than half of which are for licensing costs) as indicated in appendix three. We are preparing a Budget 22 bid and subject to your direction will develop a business case to implement a work programme from July 2022, starting with the technologies that pose the biggest risks to school operations and/or data security.

- New approaches are urgently needed and will realise significant benefits over time. The proposed changes will help free schools from the burden and complexities of IT management, leverage economies of scale, help protect schools' IT systems against service failure and data breaches, and make it easier for kura and schools to safely collaborate and exchange information.

Recommendations

We recommend you:

1. **Note** that better support is urgently needed for the many kura and schools that lack the capability and capacity to manage the growing complexities of the IT systems they rely on for their day-to-day operations;

   NOTED

2. **Note** that the Ministry, in conjunction with N4L, is implementing a range of tactical actions in this financial year to help protect kura and schools from cyberattacks and data breaches, but there is more work to be done to move towards IT systems that are safe, secure, and fit for purpose;

   NOTED

3. **Note** this paper proposes a progressive shift to centrally managed core IT infrastructure and services on behalf of kura and schools, starting with those services at greatest risk of cyber-attack, service failure and/or privacy breaches;

   NOTED

4. **Note** that policy changes will be necessary, for example to ensure kura and schools use services assured against interoperability, privacy and security standards, to require kura and schools to report cybersecurity incidents and privacy breaches, and to review the way kura and schools are funded for IT;

   NOTED

5. **Agree** in principle to transition to a more directly, centrally led managed environment for IT in kura and schools, subject to approval of an associated business case and funding;

AGREE / DISAGREE

6. **Note** that if you agree to recommendation 5, we will:
   I. prepare a programme business case by the **end of March 2022** to set out a multi-year work programme and a proposed operating model for managed services to strengthen cybersecurity and IT support starting from July 2022
   II. Prepare subsequent detailed business cases for each tranche identified in the programme case;

   NOTED

7. **Note** that we are preparing Budget 2022/23 funding bids to establish the foundations for improving IT support in kura and schools, including the 'managed choice option' for SMS and building on the tactical cybersecurity workstream;

   NOTED

8. **Note** that this paper focuses on kura and schools, and that we will send you advice by the end of October on systems settings needed to strengthen monitoring, assurance, cyber threats and incident management and recovery across the wider education sector.

   NOTED

Proactive Release

9. **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

Scott Evans

Te Puna Hanganga, Matihiko
Infrastructure and Digital

8/10/2021

Hon Chris Hipkins

Minister of Education

__/__/__

Introduction

1. On 8 June 2021 you requested a briefing on cybersecurity risks and their impacts on kura and schools. We provided advice in an education report: Initial advice on cybersecurity in kura and schools (Metis #1262630) and a further report, SMS vendor market options and recommendations (Metis #1266675).

1. In response you agreed to the Ministry providing advice on how kura and schools could be better supported with IT and agreed that a 'managed choice' solution is the most appropriate approach to deliver the required capability, quality and security uplift for school SMS services.

2. Recent cyberattacks on schools have again highlighted the risks posed to schools and kura. The lack of whole-of-system safeguards, including explicit requirements on schools to implement security protections, report incidents or provide access to their security logs, make it difficult to mitigate and respond quickly to cyber-attacks.

3. Five tactical workstreams are underway to expand cybersecurity protections:
    1. Establish offline backup capabilities for kura and schools
    2. Establish interim email protection capabilities for kura and schools
    3. Accelerate the rollout of secure access to school and kura networks
    4. Review cybersecurity insurance arrangements
    5. Run a cybersecurity awareness campaign.

4. We have secured funding for these and a project team is in place. Design work is underway on 1-3, we have begun a review of current cyber insurance, designed an education and awareness campaign and appointed a communications adviser for cybersecurity. We are seeking funding from Budget 22/23 to build out these work streams.

5. This paper provides advice that will shift the procurement and management of the most critical digital services from school boards to the Ministry, with opt-out conditions set for schools that can demonstrate they have the capability and capacity to manage their own IT. Such a shift will have significant change management, policy and funding implications, and will require several years to implement fully.

Structure of paper

Section 1: The rationale and drivers of change

Purpose

6. The approach proposed in this paper is intended to:
    1) Provide better protection to schools' IT systems against cyberattack and privacy breaches
    2) Lift the burden of IT procurement and management from boards, principals and teachers so they can focus on learning and teaching
    3) Support the vision of the Education System Digital Strategy for a safe, secure, connected and interdependent education system designed to put the needs of learners and their parents and whānau in the centre
    4) Enable system cohesion, resilience, scalability and sustainability by taking a whole-of-system approach to IT starting with the compulsory schools' sector.

7. This paper does not address how digital technologies are best used for teaching and learning or propose an approach to assessing education applications for their pedagogical value. These are outside of the scope of this paper and will be a key element of refreshing the Digital Strategy. We will provide you with further advice on refreshing the Digital Strategy at the end of October.

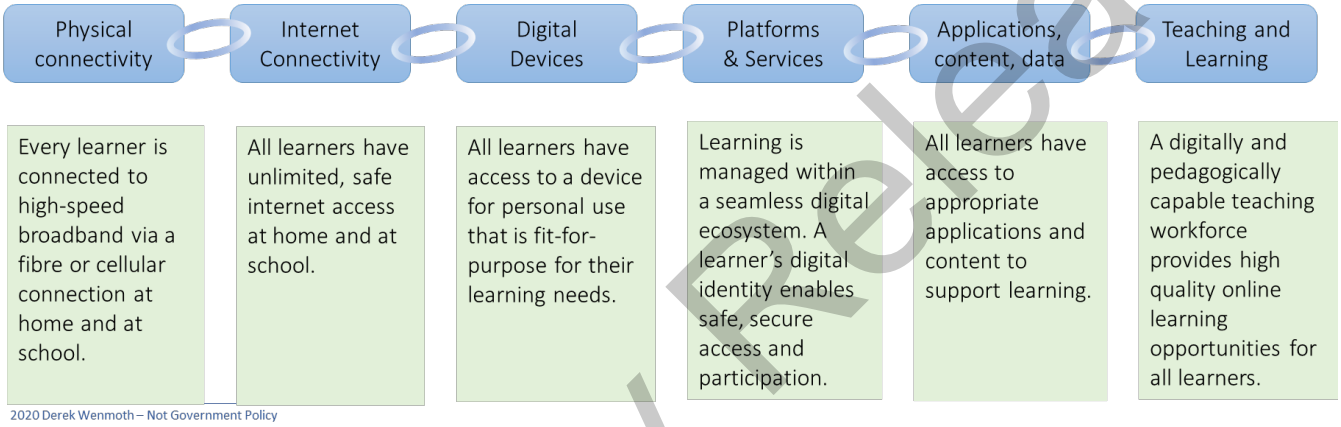
Drivers of change

8. The need for better IT support for kura and schools is driven by:
    - The urgent need to protect school systems from rising cyber threats of service failure and privacy breaches
    - Growing inequities arising from the widely variable capability of kura and schools to manage their digital environments
    - Difficulties in finding specialist IT expertise, especially in small, rural and remote areas
    - Opportunities to deploy modern digital platforms across the education system that connect the ecosystem, enhance user experience, enable collaboration and streamline administration, which requires schools to access IT providers with the capability to install and maintain cloud-based services
    - The need to ensure education continuity through disruptions such as Covid-19, extreme weather events and other emergency situations
    - Opportunities to leverage economies of scale through centralised procurement or bulk purchasing on behalf of schools

- Opportunities to enhance the maturity of New Zealand's EdTech sector by being open and transparent about the interoperability, security and privacy standards that will be required to operate in the education market.

Section 2: A digital ecosystem for New Zealand education – Taking a whole-of-system approach

9. In recent advice on cybersecurity, we referred to evidence showing that a lack of a coherent, system-wide approach to IT across the education sector is a significant barrier to the safe and effective use of digital technologies for learning. The diagram below shows the key IT elements necessary for an effective education system. A fragmented, piece-meal system impedes the effective use of technologies for learning, and where there are weaknesses or failure in any part of the system, the entire system is put at risk.



10. New Zealand is not alone in having a fragmented system. In a recent OECD address, Andreas Schleicher[1] noted that the promise of technologies to improve learning is not being fully realised in part because *"neither the industry nor public policy to date take much of an interest in an ecosystems approach to technology. We have a patchwork of solutions where the whole does not transcend beyond its parts."*

11. This paper proposes a system-wide approach to IT in the compulsory sector as a first step, with a longer-term aim to extend this across the education sector from early learning to tertiary as envisaged in the Education System Digital Strategy (2015-2020). We will provide further advice in October, focusing initially on monitoring and reducing cybersecurity risk across the sector, recognising that the approaches will need to account for the very different policy settings in the early learning and tertiary sectors.

12. Because schools have been self-managed since 1989, we have little information on the IT systems and software they use. We will do an initial needs assessment in up to 15 kura and schools during November 2021 to inform a programme business case and follow this with a more complete environmental scan in the first half of 2022 to determine the digital technologies used by kura and schools, what IT contracts they have, where the gaps are, and what causes the biggest pain points. We will inform you via the Education Weekly Update before approaching kura and schools to undertake the broader environmental scan in 2022. The scan will provide input into a **Schools' Digital**

[1] Director for the Directorate of Education and Skills for the OECD

Blueprint - a description of the necessary elements of a school's digital ecosystem and the minimum standards necessary for its safe, effective operation.

13. We will need to build the business capabilities, information and systems required to ensure successful delivery and evolution of these core digital services, including a cycle of obtaining, updating and replacing services over time, informed by ongoing monitoring and analysis. Given the speed of technology change, the Blueprint will be a dynamic rather than fixed guide for kura, schools, and the Ministry.

Section 3: A work programme to strengthen cybersecurity and IT support for kura and schools

14. This section describes the key elements of an IT support programme, which we will describe in detail in a business case by the end of March 2022 that sets out the strategic drivers and a multi-year work programme. These elements are interdependent and will need to be implemented in parallel.

    Part one: Strengthen the assurance of IT systems and applications used in kura and schools against interoperability, privacy and security standards, graduated according to the system-value and level of risk of each application.

    Part two: Lift the capability in the most critical areas starting with SMS and other IT systems and applications, such as schools' networks, that are critical to school operations and/or that store sensitive data.

    Part three: Review regulatory settings to ensure compliance with the standards, establish opt-out conditions where these can be applied, and mandate requirements to report cyberattacks and privacy breaches.

    Part four: Establish appropriate procurement and contracting arrangements, across a broad suite of services and system classes to enable the central procurement and management of core digital services to kura and schools including on-the-ground IT support.

    Part five: Provide a set of integrated digital services to kura and schools on an opt-in basis comprising the core set of functions necessary to operate safely and effectively.

15. **Appendix one** provides an early draft describing criteria that could be used to determine the nature and extent of IT support. Applying these criteria will help identify how specific digital services could be treated; which services should meet the highest interoperability and security standards, and where centrally procuring and managing services would make sense from economic, security and schools' perspectives.

Part One: Strengthen Assurance

16. As a first step we will establish an assurance framework to assess IT systems and applications used in kura and schools against agreed privacy, security, and interoperability standards.

17. Subject to policy confirmation, we expect the framework to sit within the context of existing legislation, regulations, and standards, and to support, rather than fundamentally change existing accountabilities, notably those of Boards. The framework will take a tiered approach, with the highest levels of assurance applied to the products, services and data with the highest levels of inherent risk, and will provide targeted, education sector specific guidance, accessible to the range of organisations in the sector.

18. The assurance framework will include:

    a. Core privacy, security, and interoperability expectations for education IT, including guidance on how to operate within these expectations

    b. A tiered model for establishing the level of inherent risk associated with products and services, and the associated support necessary

    c. Minimum and recommended requirements for each tier, linked to existing regulations and assessed against standards appropriate to each tier

    d. A maturity model to measure and guide uplift of sector capability

    e. A multi-layered assurance regime, incorporating assessment and assurance of individual products and services, accreditation of participating organisations, strengthened school-level practices, and system level monitoring and review

    f. Arrangements for secure sharing of assessment and assurance information

    g. Linkages to service delivery models, identification and prioritisation of products and services, procurement and commercial management. as signalled elsewhere in this paper

    h. Governance arrangements for the framework, including the accountabilities, roles and responsibilities of boards of trustees, kura and schools, the Ministry, and third parties such as IT providers.

19. The assurance activities will address both the IT systems *and* how they are used, recognising that service failure and privacy breaches are often the result of human error rather than technology failure.

20. Schools are generally not equipped to evaluate the cyber security and privacy risks of large and complex IT systems. Under these proposals the Ministry would take on a significant portion of the assurance responsibility for services with high risk or complexity, using a mix of insourced and outsourced IT providers. The level of assurance would be on a continuum, for example, the Ministry would provide guidance that schools could use to self-assess IT systems with lower levels of complexity and risk.

21. While schools will continue to be accountable for the way they use technologies and cybersecurity controls, the Ministry could provide pre-assured IT solutions and guidance on their correct deployment. We would support kura and schools to meet their accountabilities by taking more responsibility for identifying and managing risk from the centre, including in some cases centrally managing services. We would also pre-assess commonly used products and provide guidance on the risks that need to be managed by kura and schools themselves.

22. Strengthening assurance will have significant benefits beyond better cybersecurity. Data standards and interoperability between schools' and Ministry IT systems will improve the integrity of data and make data easier and safer to access, use and share. For example, integrating Te Rito with SMS will provide a verified source of a leaner's identity and their association with their education provider(s). Learner data will be accessible only to those with a right to it and will stay with the learner throughout their education.

23. We are drawing on experience in Australia of implementing a similar approach to pre-assessing IT services used in schools. We are collaborating with the intent to establish a cross-Tasman scheme based on their **Safer Technologies 4 Schools** initiative[2]. The initiative is being positively received by both schools and IT providers, and already resulting in cybersecurity improvements. A single, shared scheme will have benefits in reducing compliance costs for vendors and encouraging participation. It will also provide better value for money relative to establishing a separate scheme and enable assessment of a greater range of products and services.

Part Two: Lift capability in the most critical areas

24. A critical priority is to lift the capability of IT systems and software identified as critical to a kura and school's operation and/or that hold sensitive data. This will require improving technology capability as well as building the capability of IT providers, kura and schools to implement and use technologies safely.

Student Management Systems

25. Following our report of 29 July (Student Management System Vendor Market Options & Recommendations, METIS 1266675) you agreed to a 'managed choice' solution as the best approach to lift the capability, quality and security of school SMS services.

26. We have prepared a budget bid for Budget 2022/23 funding and will begin work on a business case for the managed choice solution that will consider options, benefits, cost estimates, implementation, change management and service delivery implications. The business case will consider how far and how fast we implement change, including testing how we manage the scale of market disruption.

27. Improving the delivery of SMS is just one aspect of the work needed to support kura and schools' IT and is dependent on that broader work programme, such as establishing the assurance framework. Addressing SMS is a challenging place to start, but time is of the essence. The nature of sensitive information in school SMS and the extent to which SMS are relied upon within kura and schools, is exacerbated by the potential fragility[3] of some SMS vendors.

28. We can draw on experience to date with the Te Rito SMS security and privacy assessment process and the Assembly SMS transition. We will directly associate Te Rito integration with improvements in cybersecurity, noting that Te Rito integration also provides an independent back-up of SMS information.

---

[2] Referenced in a Briefing note, 28 Feb 2020: Te Rito proactive launch opportunities and associated education data protection policy work, Metis 1214953

[3] 9(2)(b)(ii)

29. **The 4-year costs are estimated to total** 9(2)(f)(iv) **operating expenditure[4].** At the completion of the work programme, we expect ongoing costs of approximately 9(2)(f)(iv) 9(2)(f)(iv)

30. We are moving as quickly as possible to change the settings in which SMS vendors and schools operate but the change required is significant. Addressing the SMS vendor market will require a 4–5-year work programme that includes revising the contracts for the SMS used by kura and schools, and progressively remediating security risks.

31. In the meantime, we expect the tactical responses underway, along with Te Rito secure integration as a landing stage, to help reduce the short to medium term risks.

Schools' cybersecurity and network management services

32. Beyond the network services provided through N4L, many foundational IT services are procured by kura and schools directly from IT providers, with little or no guidance from the Ministry. The provider systems are of variable quality and their products or services are not required to be assured against common standards.

33. We have tactical workstreams underway to provide data backup services, protect in-bound email, segregate school networks to protect critical services, review cybersecurity insurance and increase cybersecurity awareness. A project team has been established and work has started on requirements and design. These workstreams will provide opt-in capabilities using existing and potentially new platforms to enable rapid deployment. We are seeking funding from Budget 22/23 to continue these tactical workstreams.

34. In addition to the tactical responses, we will need further investment to strengthen school networks, protect critical IT systems, and improve cybersecurity support and response. Te Mana Tūhono is providing a secure managed network for schools. Additional investment is required to accelerate the rollout, extend network coverage within each school (e.g., to exam spaces and outdoor areas used for learning), improve the protections provided for staff and students when working or learning off campus, and enhance the level of support for resolving school network issues.

35. We will need to better identify and protect kura and school IT systems and the devices they are being accessed from. We will establish secure configurations for commonly used, critical platforms such as office productivity suites, so that they can be used safely by schools "out of the box". We will extend this approach over time as we learn more about the higher risk and system-critical platforms through the assurance process described in paragraphs 17-24. We will strengthen the management of end-user devices (e.g., improving malware protection) and we are seeking funding from Budget 22 to improve the identification of end-users through extending Digital Identity for Online Learning (DT4OL) to all kura and schools.

36. We will also need to improve sector cybersecurity support and response capability. We will expand the scope of cyber security operational monitoring of school systems, such as emails and office productivity usage, to better detect cyber threats. We will provide

[4] $16.7m departmental, and $41.4m non-departmental operating expenditure.

increased cybersecurity awareness training and support and consider the need for incident response teams.

37. To achieve significant improvements in cybersecurity for kura and schools, uptake of these improvements will be critical. We will need to identify incentives and support to achieve maximum uptake. We will need to review the compliance obligations on kura schools, especially where they implement their own solutions or do not chose to adopt the cybersecurity improvements offered centrally.

38. Cyber-safety is linked to cybersecurity and is reported by secondary school principals to be one of the major issues they face[5]. A review of cyber-safety for schools will be necessary, with changes to ensure controls that address both cyber-safety and cybersecurity.

Part Three: Review regulatory settings

39. A move towards greater support for kura and schools' IT will have implications for decision-making, roles, responsibilities, liabilities and obligations of the Ministry, boards of trustees, IT providers and other agencies. If you agree to our proposals, we will review existing legislative settings and their application and suitability, including whether further legislative or regulatory settings are needed for effective implementation.

40. Since 1989 kura and schools have become used to exercising autonomy over much of their decision-making and many expect to be able to opt-out of settings where they believe it to be in their interests to do so. Given the critical importance of protecting kura and schools from service failure and privacy breaches, we will need to consider settings for compliance, including how to monitor and ensure compliance and what conditions could be set that allow kura and schools to opt-out of centrally delivered services.

41. Our aim would be to make solutions attractive so that there would be considerable value in opting-in and complying with requirements. 9(2)(g)(i) 9(2)(g)(i)

    - Other value propositions that would incentivise compliance such as reducing teacher and principal workload, improving security, and taking on some of the cyber risk currently carried by boards.

42. Should we require regulation, we can apply Section 638 of the Education and Training Act 2020 (E&T Act) which allows the Governor-General to make regulations providing for the control, management, organisation, conduct, and administration of schools. We have looked at other possible Acts outside education but believe we can achieve what we need under the E&T Act, which also allows us to adjust regulations through our legislative process should it be needed.

[5] Secondary Principals reported "Dealing with inappropriate use of technology" as the 7th major issue they face. NZCER_Nat-Survey-Report-Secondary.pdf page 144.

Part Four: Establish appropriate procurement and contracting arrangements

43. The guide to decision making in appendix one signals the need for a range of procurement and contracting arrangements appropriate to the digital services used by schools. We will explore options as part of the business case, which may include the Ministry:
    - Centrally procuring and managing core services critical to school operations and/or that handle sensitive data
    - Establishing managed panels, such as we are proposing for SMS, which gives schools a choice of assured services
    - Bulk purchasing services on behalf of schools, such as we do for Google and Microsoft software
    - Leveraging AoG procurement arrangements.

44. Implementing any of these options will have impacts on IT providers, which we note in paragraphs 48-51. The lack of capability of some IT services used by kura and schools is a key driver for the need to intervene and ensure they can access services that are safe, secure and fit-for-purpose.

Part Five: Provide integrated, bundled digital services

45. As we transition to cloud-based technologies it will be possible to create a fully integrated digital ecosystem for education, which we intend to build through years 3 and 4 of the work programme. This will have significant benefits for kura and schools, including streamlining classroom and school administration, enabling the secure flow of data, and making collaboration within and beyond schools easier. We have included a description of what this might look like at **appendix two**.

46. Over time we anticipate being able to provide kura and schools that opt-in with a set of integrated bundled services that comprise an office productivity suite, digital identity provider, accounting and HR software and other core services.

Section 4: Change implications

Implications for funding of kura and schools

47. Kura and schools fund their IT from various sources including new-build funding, furniture and equipment grants, operations grant, parental donations and fundraising, board of trustees and community sources such as trusts. Operations grant funding is not tagged and it is difficult to know with any accuracy the amount spent on IT.

48. We know that the cost of technology tends to rise, not least as kura and schools struggle to keep pace with community expectations for increased use of technology and access to information. There is also the rising complexity of technology and the risks associated with its use. Also, the real cost of IT in kura and schools is often hidden as many use free and trial software, often without realising the considerable risk of the misuse of personal information, and that the failure to establish security standards means that the true cost of an assured IT ecosystem is not appreciated.

49. The Ministry already provides a range of services at little or no cost to schools including, but not limited to:
    - Managed network services through N4L
    - The TELA laptop scheme
    - Hardware upgrades through Te Mana Tūhono
    - National contracts with Google and Microsoft for office productivity suites.

50. These services total approximately $78M p.a. In addition, we have allocated $6M in the current financial year to strengthen cybersecurity in kura and schools.

51. The proposals in this paper will expand the digital services centrally provided to kura and schools and will require investment. Further work is needed to identify the core digital services necessary for schools to operate safely and securely and what these will cost. We will explore funding options through the business case, which could include fully funding core digital services or drawing funding from kura and schools' operations grants to help offset costs. A key consideration will be incentivising schools to use the services provided, rather than low-cost or free services that put their data and operations at risk.

Impacts on the IT provider market

52. The cybersecurity framework provides an opportunity to progressively lift the capability of education IT services through a maturity model of cybersecurity. By establishing where each service sits on the continuum of cybersecurity standards, including how it is assured or supplied, vendors will be required to meet the base standards and demonstrate their capacity for ongoing improvement.

53. In the early phases, many vendors will need time and investment to meet the minimum standards. We propose providing some support to vendors to lift capability, rather than risk a denial of service to kura and schools or create additional pressure on them to move to another provider.

54. We anticipate that some vendors will see this as an opportunity to upgrade their systems; others may view the time and investment need to bridge the gap as too high and retreat from the market. We would need to manage the risk of those vendors unable to reach the standards creating disruption to the kura and schools using their services.

55. A drive to lift cybersecurity capability in compulsory sector SMS vendors will send a clear signal to vendors of other education services of the need to do the same, e.g., SMS providers in early learning and tertiary, and providers of digital services such as LMS. The experience of the Safer Technology 4 Schools initiative in Queensland indicates that the EdTech sector welcomed having clear standards to meet and a transparent process.

Financial implications

56. There are significant costs associated with uplifting the capability of the digital services identified in this paper which are described in **appendix three**. The total of 9(2)(f)(iv) over 4 years is an estimate based on what we have identified to date but still has a wide potential range depending on factors including uptake by schools and how varied each kura and school's needs are. We anticipate a range of between 9(2)(f)(iv) fully

costed over 4 years. These costs will be refined as part of the business case analysis and environmental scan which will increase the accuracy of our estimates.

57. We have identified that more than half of the estimated costs are for the provision of cloud services, software subscription and licensing, and increased funding to existing service providers, not for workforce effort.

58. In line with guidance issued by the Government Chief Digital Officer, the capability uplift will have a preference towards cloud technologies which are costed on operating expenditure.

Consultation and communication

59. These proposals will see a significant shift toward central oversight of kura and school IT services which is likely to get a mixed reaction from the sector and IT providers. Our focus will be on the many kura and schools that struggle with IT and will welcome the support, but the cybersecurity and privacy risks are such that a level of central mandating of core digital services accredited against appropriate IT standards is likely to be necessary.

60. Two initiatives are underway that will provide opportunities to engage with kura and schools, the tactical responses to cybersecurity threats which includes an education and awareness campaign, and the refresh of the Education System Digital Strategy, which will be consulted on during 2022 under the direction of the cross-agency Education Digital and Data Board. Further advice on refreshing the Digital Strategy is due to your office by the end of October.

Section 5: Implementation – next steps

61. We expect the proposed work programme to take several years to implement, followed by a rolling programme of maintenance, upgrades and introduction of new technologies.

62. As an immediate step, we are seeking up to $32.35M from Budget 2022/23 to enable the Ministry to:
    - **Strengthen the assurance** of IT systems and applications used in kura and schools against interoperability, privacy and securing standards, graduated according to the system-value and level of risk of each application.
    - **Lift the capability in the most critical areas** starting with the core IT systems and software, including SMS
    - **Expand the managed network services** we make available to schools via N4L to build on the tactical responses to cyber threats being implemented in this financial year.

63. It will take time for the design and planning necessary to establish the assurance framework and lift the capability of core systems including SMS. The amount needed in 2022/23 is relatively modest but will rise incrementally in the following three years during which we will revise the contractual arrangements with SMS vendors and IT providers; lift the capability and manage the change at school and vendor level.

64. Ministry involvement in the supply, oversight and regulation of kura and schools' IT systems will need to be managed with transparency and co-designed with the sector. Te

Rito has surfaced concerns about trust, particularly in relation to learner data, leading to the creation of a sector data oversight group (Te Rito Kaitiakitanga) and defining the Ministry's role as a 'service agent' providing Te Rito as a service to schools. We will explore the extent to which the Ministry's proposed service agent role for data held in Te Rito could provide a basis for our approach to managing core digital services on behalf of schools.

65. The change management will be significant. The migration from current to future IT providers will be the largest transition of IT services and student data in the education sector to date. We will need to establish new procurement, contracting, service management and security standards across a broad suite of services and system classes.

66. The Ministry's design and implementation approach will be elaborated in a business case we will draft subject to your agreement to the proposals in this paper, in preparation for a start in July 2022. This will include a high-level approach to governance and management of the cybersecurity framework, which will introduce new roles and responsibilities for the Ministry, kura, schools, boards of trustees and IT providers.

67. Right now, work is underway on tactical measures to improve cybersecurity in kura and schools, and this paper proposes a more comprehensive work programme to support IT in the compulsory schools' sector. We also are exploring how to strengthen cybersecurity across the broader education system from early learning to tertiary. We will provide you with advice in late October on the system-wide settings required to strengthen monitoring, assurance, cyber threat and incident management and recovery across within education agencies and the wider sector.

Appendix One: SUPPORTING KURA AND SCHOOLS – CRITERIA TO GUIDE TO DECISION MAKING (Early draft only - not government policy)

These quadrants recognise that:

- Kura and schools use a wide range of IT solutions. While some are tailored to specific needs, others could be centrally provided to all kura and schools.
- Greater support for school's IT would help relieve boards of both the cost and management burden, and provide economies of scale, e.g., through bulk purchasing arrangements

The quadrants use two key variables to help guide investment and management decisions:

- **RISK** – how significant are the risks of cyber-security threats, privacy breaches or service failure?
- **SYSTEM VALUE** – how critical is this service to a digitally-enabled education system? What level of value does it provide to the system as a whole? NB – low system value does not imply low value per se – an individual school may still find a particular service or application of high value to them.

Some solutions will lie clearly within a specific quadrant, others may sit at or across the boundaries.

The criteria and examples are indicative only, based on what we know and consultation with a small sample of schools, and will need further co-design with the sector.

Those consulted agreed their biggest challenge is managing the risk around student and school data, and the security risks associated with Internet filtering, and identity and access management.

Applying these criteria would help make decisions about:

- The procurement and management arrangements most appropriate to each service
- The degree to which kura and schools can choose; services such as SMS may be mandated unless strict opt-out conditions are met
- The appropriate level of accreditation or assurance against interoperability, privacy and security standards for each service.

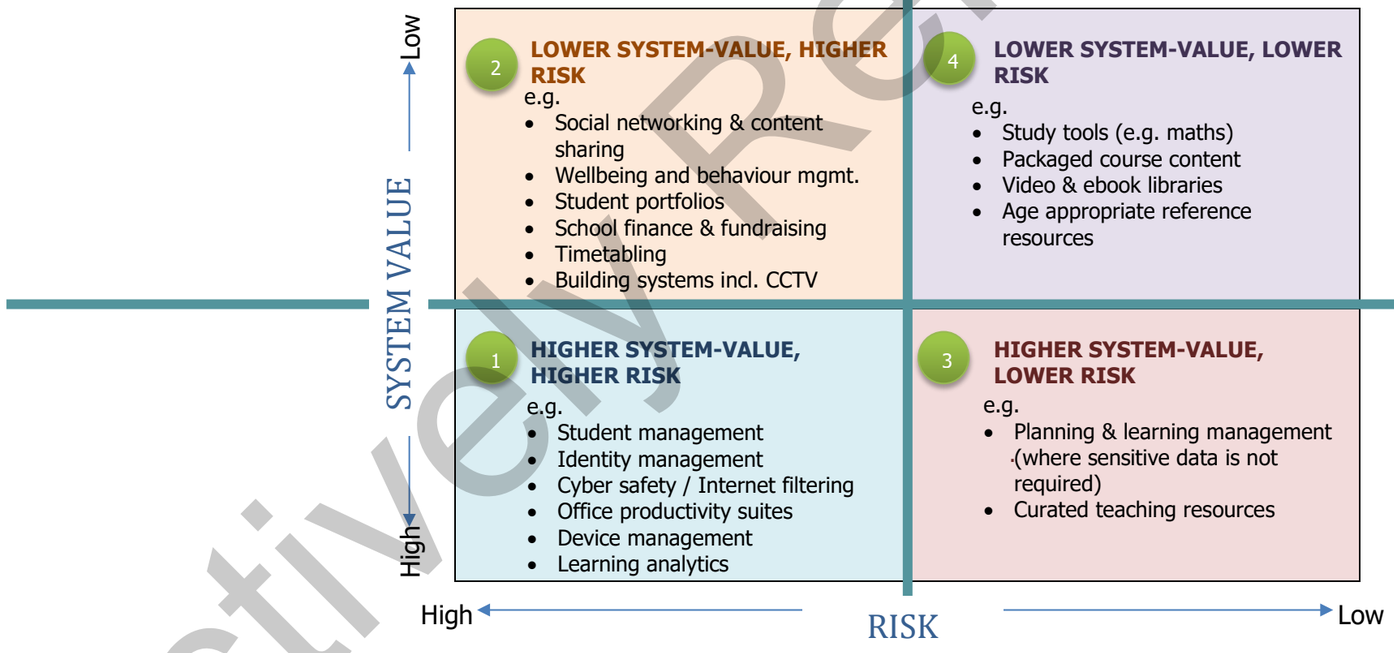
- Non-core (non-critical) requirement.
- Holds sensitive data about individuals.
- High impact on school/cluster business systems.
- System benefits from high volume licensing and support.
- High value in local/specialised needs.
- High risk from vendor failure.

Services…

- Are best suited for local contexts and addressing specialised needs.
- Most likely to be selected for use at a local level from a suite of providers.
- Must meet all the requirements in an approved assurance process.

Schools may be audited as part of the regular review process to ensure they are using approved services.

- Non-core (non-critical) requirement.
- High value in local/specialised needs.
- Limited/no sensitive data about individuals kept in the system.
- Enables agile, responsive and adaptive (localised) curriculum support.
- System benefit from having multiple providers (innovation, responsiveness, user preferences)
- Limited/no data stored about individuals
- Low cost for licensing/support
- A lot of choice in the market - low risk from vendor failure
- Not security critical
- Multiple providers in the market
- Providers self-assess against the assurance criteria and will be open to being audited on request.
- Schools use publicly accessible assurance criteria to guide their choice.



- Core (critical) system requirement.
- Holds sensitive data about individuals.
- Lack of choice for viable options.
- Security is critical (e.g. IAM/idp, perimeter security, end-point protection etc.)
- May be highly customised to NZ context (e.g. SMS based on NZ reporting requirements)
- High impact on business systems.
- System benefits from high volume licensing and support.
- Provides high value system level insights.
- Enables system level sustainability and scalability.

Services…

- May be centrally procured and supported.
- May be mandated for use by all schools.
- Must meet all the conditions of an approved assurance process.

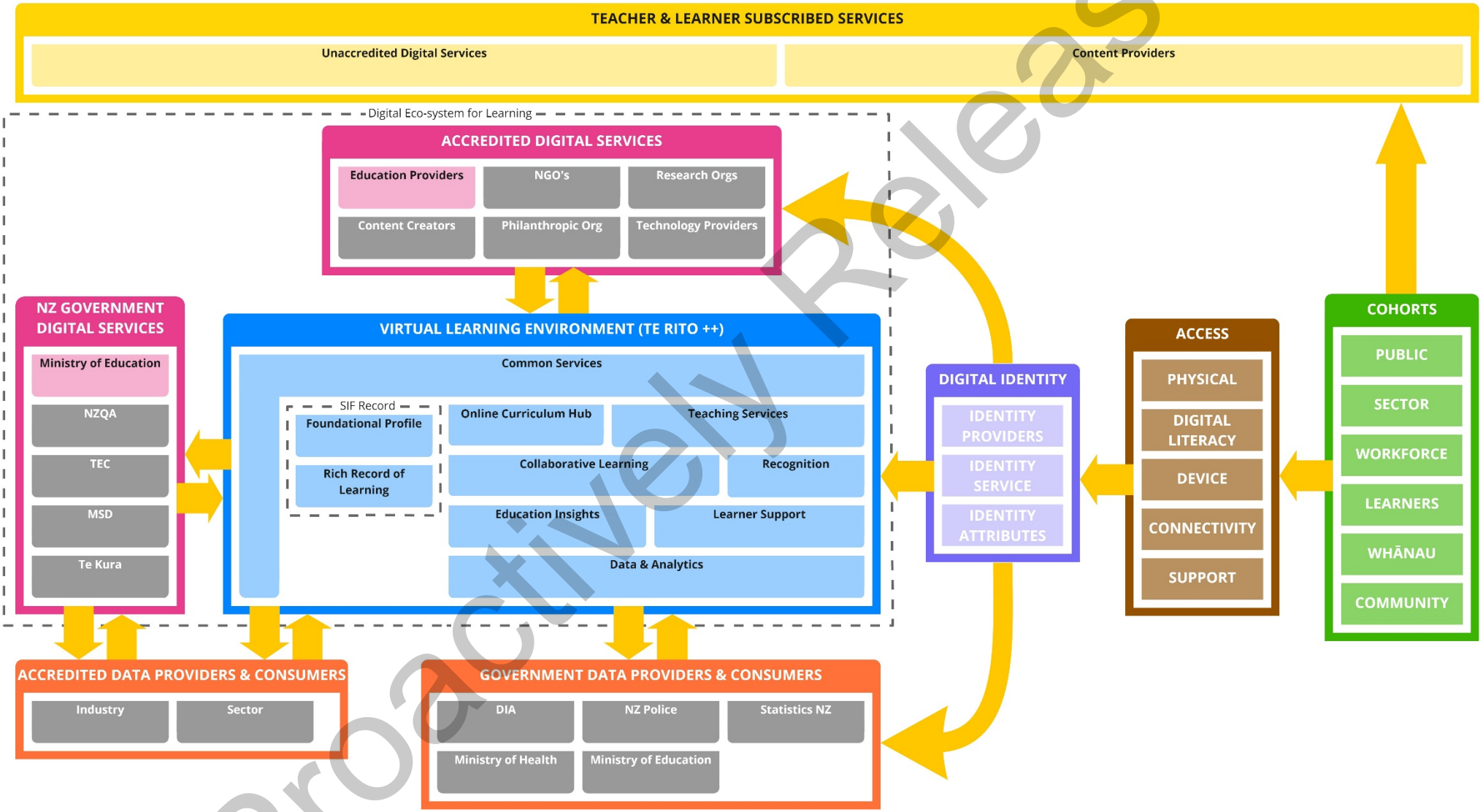
- High value (critical) system requirement.
- Sensitive data held/managed externally.
- Low risk from vendor failure.
- Addresses equity gaps.
- Enables student/whānau centred system.
- May be multiple services in this quadrant that provide choice in areas of essential/critical system functionality.

Services…

- Must meet of the requirements of the approved assurance process.
- May involve (all/some) central procurement and funding.

Appendix Two: KEY ELEMENTS OF A DIGITAL ECOSYSTEM FOR LEARNING

This diagram provides a high-level view of the Virtual Learning Environment (VLE) showing the services required to support a safe, secure, effective digital ecosystem for learning. The ecosystem will deliver integrated services that can be trusted and valued by New Zealand teachers and learners. It is founded on core principles, standards and digital services necessary to operate effectively and will enable all education cohorts to assert their identity in a trusted way. Applying common standards will enable public and private organisations to integrate their own service offerings with the appropriate assurance.



Appendix Three: FINANCIAL SUMMARY

	Year 1 ($m)	Year 2 ($m)	Year 3 ($m)	Year 4 ($m)	Total ($m)	Ongoing ($m)
Part One: Strengthen Assurance						
Assurance framework for digital services						
- Capital expenditure	9(2)(f)(iv)					
- Operating expenditure						
Part Two: Lift capability in the most critical areas						
Student Management Systems						
- Capital expenditure	0	0	0	0	**0**	0
- Operating expenditure	9(2)(f)(iv)					
Schools' cybersecurity and network management services						
- Capital expenditure						
- Operating expenditure						
Part Three: Establish appropriate procurement and contracting arrangements						
Assurance framework for IT providers						
- Capital expenditure	9(2)(f)(iv)					
- Operating expenditure						
Part Four: Review regulatory settings						
Policy development						
- Capital expenditure	0	0	0	0	**0**	0
- Operating expenditure	0	0	0	0	**0**	0
Part Five: Provide integrated, bundled digital services						
Primary service offering						
- Capital expenditure	9(2)(f)(iv)					
- Operating expenditure						
Totals						
- Capital expenditure						
- Operating expenditure						
Total expenditure						