Dr. James Curran
CEO and Director

15 April 2023

To Whom It May Concern,

RE: SUBMISSION TO THE GOVERNMENT DISCUSSION PAPER ON CYBER SECURITY

Grok Academy is the leading edtech not-for-profit in Digital Technologies and cyber security education for primary and secondary students. Our submission is focused on the **critical need for cyber security technical skills and dispositions development *throughout schooling***.

My colleagues and I wrote the Australian Curriculum: Digital Technologies (v8 and v9) and the Digital Literacy (v9) general capability. V9 includes content on cyber security and privacy knowledge and skills (ranging from unique passwords to threat modelling) for the first time. The full list of content descriptions on security are included below.

Grok works closely with federal and state Departments of Education, the Catholic and independent school sectors, and industry partners to implement this new curriculum across all Australian schools.

We aim to *educate all learners in transformative computing knowledge, skills and dispositions, empowering them to meet the challenges and seize the opportunities of the future*. We appreciate the opportunity to contribute to the government's discussion paper on cyber security strategy, focusing on three core aspects:

1. A secure economy and thriving cyber ecosystem;
2. A sovereign and assured capability to counter cyber threats; and
3. Australia as a trusted and influential global cyber leader.

1. A secure economy and thriving cyber ecosystem

The foundation of a secure economy and thriving cyber ecosystem is an educated workforce. We recommend the government prioritise widespread cyber security education in primary and secondary schools across Australia. This requires:

- classroom activities that:
  - support the Australian Curriculum: Digital Technologies and Digital Literacy;
  - increase awareness of the range of cyber security careers and paths; and
  - extend talented school students in cyber security.
- extensive and widespread cyber professional development for our 350,000 teachers.

We must invest heavily in every blocker of effective DT/DL education in schools, including the technical and pedagogical skills of educators, and devices and infrastructure so that every Australian child has the opportunity to develop advanced digital and cyber skills.

Working with industry

We encourage the government to support initiatives that promote collaboration between the educational ecosystem, industry, and government agencies.

Grok Academy Limited
Level 1, 130-144 Cleveland Street
Chippendale
NSW 2008 Australia

[redacted]
W grokacademy.org

ABN 31 643 542 054

Grok has developed an effective collaborative model for creating resources and activities to support teachers in teaching cyber security – the *Schools Cyber Security Challenges*.

Our current industry partners are ANZ, AWS, BT, CBA, Fifth Domain, NAB, and Westpac. Our government partners are AustCyber, Australian Signals Directorate, and the Department of Industry, Science, and Resources.

We collaborate closely with partner subject matter experts to design online *Cyber Challenges*, that are aligned to the AC:DT. The Challenges involve interactive learning activities, assessment, and intelligent, automated feedback in the Grok platform. The learning material is presented by partner SMEs.

We embed 1-2 min career videos so that students can see, and get a taste for, the opportunities and roles available in the sector. After a student discovers that they may have an interest and talent for cyber security, they hear from experts who enjoy this work every day.

This very successful model has enabled **over 250,000 students (since 2019) to learn cyber security skills, dispositions, and careers in depth**. This is one of the largest (per capita) cyber security school programmes in the world.

Our government partners – ASD, AustCyber, and DISR have been critical to the success of this programme. They not only provide expertise and financial support, but they demonstrate to (potential) industry partners that government is strategically aligned and sees the importance of cyber education in schools.

We recommend that government agencies, especially ASD, see growing the cyber skills pipeline from primary school onwards, be a central part of their long-term objectives. These skills are essential for all students, regardless of their career goals. It is also essential for growing the pipeline into cyber security careers.

2. A sovereign and assured capability to counter cyber threats

A critical part of "sovereign" capability is the skills and dispositions of *Australian citizens*. To be truly effective, these skills and dispositions must be developed from primary school.

Australia now has a world-leading Australian Curriculum: Digital Technologies (v9) that includes explicit teaching of cyber security and privacy skills. DT includes that students can:

- **Foundation**: identify some data that is personal and owned by them;
- **Year 1-2**: access their school account with a recorded username and password;
- **Year 1-2**: discuss that some websites and apps store their personal data online;
- **Year 3-4**: access their school account using a memorised password and explain why it should be easy to remember, but hard for others to guess;
- **Year 3-4**: identify what personal data is stored and shared in their online accounts and discuss any associated risks;

- **Year 5-6**: access multiple personal accounts using unique passphrases and explain the risks of password re-use;
- **Year 5-6**: explain the creation and permanence of their digital footprint and consider privacy when collecting user data;
- **Year 7-8**: explain how multi-factor authentication protects an account when the password is compromised and identify phishing and other cyber security threats;
- **Year 7-8**: investigate and manage the digital footprint existing systems and student solutions collect and assess if the data is essential to their purpose;
- **Year 9-10 (elective)**: develop cyber security threat models, and explore a software, user or software supply chain vulnerability; and
- **Year 9-10 (elective)**: apply the Australian Privacy Principles to critique and manage the digital footprint that existing systems and student solutions collect.

V9 was endorsed on 1 April 2022 by education ministers. States, territories, Catholic, and independent school sectors will implement the curriculum over the next few years.

2023-2026 is *the critical time* for large-scale professional development for teachers. The vast majority need to develop cyber skills themselves so they can pass them onto students.

Grok Academy has demonstrated that government investment in early cyber security education, especially teacher cyber skills and classroom resources, is critical to providing students with the foundational knowledge and skills required for a career in cyber security.

This investment will help create a future generation of skilled professionals capable of defending Australia against cyber threats.

Our Cyber Challenges allowed Grok to demonstrate that **cyber security skills (as distinct from cyber safety) could be taught effectively without expert teachers** and there was **demand for cyber skills from students, teachers, and parents.** This gave us the evidence base to push for the significant increase in cyber security and privacy in the Australian Curriculum v9.

For Australia to be protected, ultimately every Australian needs to have these skills and dispositions. School remains the best place for every Australian to develop these.

3. Australia as a trusted and influential global cyber leader

Australia has the potential to become a global leader in cyber security education, working alongside our neighbours to build a cyber-resilient region. We have a curriculum that is world-leading and we now must back it up by developing and evaluating a range of national education programmes to support the curriculum. We can then export the best of these worldwide.

It is also imperative that government invest in programmes that support the development of cyber security capacity in neighbouring countries, including New Zealand, the Pacific nations, and South-East Asia.

Dr. James Curran
CEO and Director

Grok Academy is committed to working with the government to deliver educational programs tailored for primary and secondary students in these countries, fostering a culture of cyber security awareness and resilience from a young age, and in fact is already doing go.

Our Cyber Skills Aotearoa online programme for schools in New Zealand has been developed in both English and Māori, based on our highly successful Cyber Challenges in Australia.

We are partnering with the NZ government (Department of Prime Minister and Cabinet, Ministry of Education, CertNZ, and N4L) and industry partners: ASB, AWS, and BNZ. The cyber content is developed in conjunction with Māori-medium education partner, CORE Education.

We recommend that DFAT and other agencies consider cyber security education as a critical activity for Australia to both export and make available to developing neighbours.

Our experience in NZ demonstrates both the need and our ability to create localised versions of cyber (and broader digital) education activities. This is not only good diplomacy, but we believe we have an obligation to train everyone on this front, especially our nearest neighbours, in these skills and disposition.

4. Summary

- 2023-2030 is a critical period for strategic investment in cyber education in schools.
- The Australian Curriculum (v9) is world-leading on cyber skills and dispositions.
- We need widespread cyber professional development for teachers and scalable classroom activities for the curriculum to be implemented effectively.
- Grok has developed a successful partnership model for these with over 250,000 students engaged since 2019.
- This model can be exported and made available to our international neighbours.

By effectively integrating cyber security education into the national curriculum, establishing a future generation of skilled professionals, and fostering international collaboration, we are confident that Australia can build a secure economy, develop a sovereign capability to counter cyber threats, and become a trusted and influential global cyber leader.

We look forward to the government's response to our recommendations and are ready to support the implementation of a comprehensive national cyber security strategy.

If you have any questions about our submission, feel free to ring me on [redacted] or email [redacted]

Yours sincerely,

[redacted]

Dr. James Curran
CEO and Director

Grok Academy Limited
Level 1, 130-144 Cleveland Street
Chippendale
NSW 2008 Australia

[redacted]
W grokacademy.org

ABN 31 643 542 054