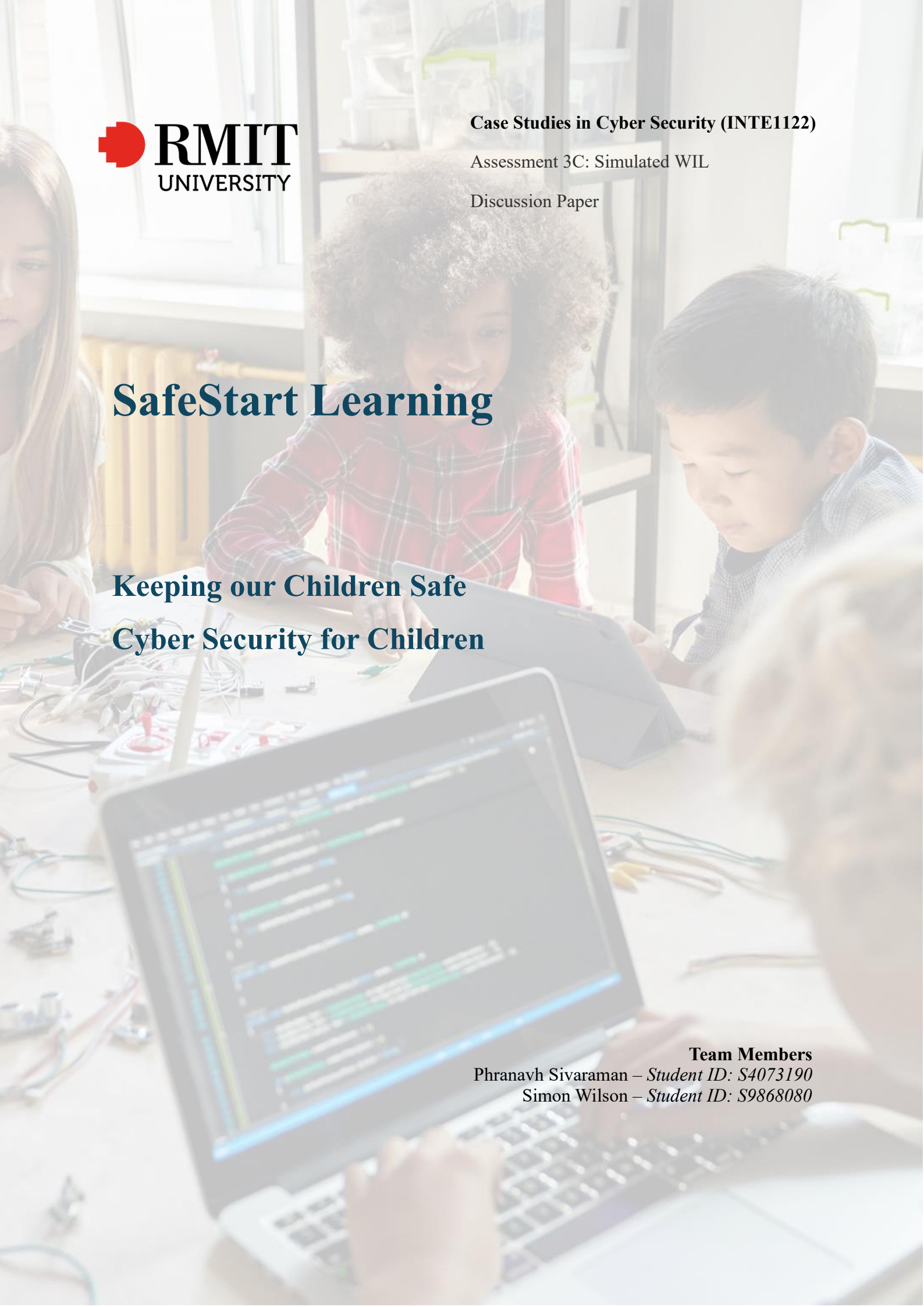


RMIT UNIVERSITY

Case Studies in Cyber Security (INTE1122)

Assessment 3C: Simulated WIL

Discussion Paper

SafeStart Learning

Keeping our Children Safe

Cyber Security for Children

Team Members

Phranavh Sivaraman – *Student ID: S4073190*

Simon Wilson – *Student ID: S9868080*

Contents

Executive Summary

In an increasingly digital learning environment, children are more exposed than ever to online threats such as data breaches, cyberbullying, grooming, and online scams. For *SafeStart Learning,* a private educational provider specialising in early childhood and primary education, these threats present not only a risk to student welfare but also to regulatory compliance, institutional reputation, and parental trust (UNICEF 2017; eSafety Commissioner 2025).

Children's developing cognitive abilities and limited digital literacy make them especially vulnerable to cyber threats. Educational institutions that fail to implement adequate digital protections risk breaching obligations outlined in key regulations such as the *Privacy Act 1988*, the *Child Safe Standards*, and the *eSafety framework* (Office of the Australian Information Commissioner 2025; Commission for Children and Young People n.d.; eSafety Commissioner 2025). Non-compliance can lead to severe consequences, including legal liability, financial penalties, and reputational damage.

This discussion paper identifies the specific cybersecurity risks facing children in school settings and outlines a strategic response tailored for *SafeStart Learning*. Key recommendations include enforcing a controlled Bring Your Own Device ("BYOD") policy or issuing secure school-managed devices, implementing enterprise-grade Wi-Fi encryption with real-time content filtering, and delivering targeted cyber safety education for students, staff, and families (Australian Cyber Security Centre 2024; eSafety Commissioner 2025).

To detect and respond to threats such as cyberbullying or grooming, the paper also recommends deploying monitoring and alert systems integrated with a formal incident response plan. Furthermore, governance-level measures are essential. These include appointing a dedicated Cyber Safety Officer and forming a Cybersecurity Governance Committee to oversee compliance, risk assessment, and continuous improvement (AICD 2024).

By acting decisively, *SafeStart Learning* can demonstrate leadership in digital child protection, ensure regulatory compliance, and enhance stakeholder confidence.

Background and Context

The Digital Lives of Children

The modern childhood experience is deeply entwined with digital technologies—from interactive tablets and gaming platforms to messaging apps and video-sharing services designed for older audiences (Holloway, Green & Livingstone 2013). Today, children use internet-enabled platforms for education, entertainment, and social connection, often without adult supervision. In Australia, over 90% of children aged 5–14 access the internet regularly, frequently via smartphones, school-issued tablets, or shared home devices (eSafety Commissioner 2025). While this connectivity promotes learning and digital inclusion, it also creates a spectrum of cybersecurity vulnerabilities.

Children's limited digital literacy and natural curiosity make them particularly susceptible to malicious content, online grooming, scams, and misinformation. Additionally, their digital activities generate significant volumes of sensitive information—email addresses, location metadata, behaviour logs, and learning analytics—that, if improperly secured, can be exploited by cybercriminals or result in data privacy breaches (Witzleb & Paterson 2020; Zhao et al. 2019). Thus, cybersecurity in this context extends beyond technical configurations—it is a fundamental aspect of holistic child protection.

Role of Educational Institutions in Digital Safety

Educational institutions are no longer passive enablers of technology but are now frontline guardians of children's digital wellbeing. Schools are expected to maintain age-appropriate, secure, and privacy-compliant learning environments (Australian Cyber Security Centre 2024). These obligations are codified in national frameworks such as the *Privacy Act 1988*, *Child Safe Standards*, *eSafety Guidelines*, and digital conduct policies mandated by state departments (Office of the Australian Information Commissioner 2025; Commission for Children and Young People n.d.; Department of Education 2025).

Failing to meet these requirements exposes schools to significant risks—legal liability, reputational damage, regulatory fines, and loss of parental trust (Grande, Pore & Elesio 2025). A single cyber incident can erode public confidence built over years. As highlighted by Waller (2017), school communities increasingly expect proactive digital safety governance as part of their broader duty of care.

To adapt, institutions must adopt a strategic, systems-level approach—investing in secure digital infrastructure, implementing strong governance practices, and fostering digital resilience across students, staff, and parents alike. Only then can they ensure every child's digital journey remains not just inclusive—but safe and empowering.

Cybersecurity Threat Landscape for Children

Data Privacy Breaches

Children are often unaware of the consequences of sharing personal information online, making them especially vulnerable to data privacy breaches (Zhao et al. 2019). Threat actors exploit this by targeting educational platforms and applications that collect sensitive student data such as names, addresses, photos, medical history, and behavioural records. A breach of such data not only exposes children to identity theft and digital surveillance but also puts educational institutions at risk of non-compliance with the Privacy Act and the Australian Privacy Principles ("APPs") (Office of the Australian Information Commissioner 2025).

Cybercriminals may sell or misuse student data, and breaches can have long-term psychological effects on children who may not fully comprehend the scope of the incident (Shen 2017). Moreover, the reputational damage to schools is significant, with parents losing trust in institutions that fail to protect their children's privacy.

Cyberbullying and Online Harassment

Cyberbullying is one of the most pervasive online threats faced by children. It includes actions such as spreading rumours, sending threatening messages, and deliberately excluding individuals from online communities. Unlike traditional bullying, cyberbullying can occur 24/7 and often leaves digital traces that continue to impact the victim even after the incident ends (eSafety Commissioner 2025).

In Australia, over 1 in 5 students report experiencing cyberbullying, with impacts ranging from anxiety and academic decline to self-harm and depression (Commission for Children and Young People n.d.). Schools are often the first point of contact for concerned parents and students, yet many institutions lack the infrastructure and trained personnel to monitor, detect, and respond effectively to such incidents.

Scams, Grooming, and Social Engineering

Online grooming and scam attempts are especially dangerous for younger users who may not understand social engineering tactics. Groomers often pretend to be peers or authority figures to gain trust, extract personal information, or arrange in-person meetings with malicious intent (Whittle et al. 2013). These incidents are frequently underreported due to fear, shame, or the child's failure to recognise inappropriate behaviour.

Similarly, phishing and scam messages targeting children may involve fake game tokens, app subscriptions, or contests asking for login details or payment information. Without appropriate safeguards and digital literacy, children can unknowingly compromise their security or expose school networks to broader attacks (Australian Cyber Security Centre 2024).

Exposure to Inappropriate Content

Children can also inadvertently access violent, sexually explicit, or otherwise harmful content online (Wold et al. 2009). Despite content moderation technologies, algorithm-driven platforms like YouTube or TikTok may still serve inappropriate material based on user behaviour, making real-time content filtering a necessity (eSafety Commissioner 2025).

The emotional and psychological consequences of such exposure can be long-lasting, especially for early learners. Schools have an ethical and regulatory duty to ensure that internet access provided on campus is filtered, age-appropriate, and actively monitored. Failure to do so may result in breach of duty under the Child Safe Standards and related educational regulations (Commission for Children and Young People n.d.).

This threat landscape highlights that cybersecurity is not only about preventing external attacks but also about creating a safe digital environment for vulnerable learners. The following sections of this paper propose realistic, resource-conscious strategies that SafeStart Learning can adopt to address these issues while complying with regulatory obligations.

Business and Legal Implications for SafeStart Learning

Regulatory Compliance: Privacy, Safety, and Legal Expectations

SafeStart Learning operates in a highly regulated space where failure to meet cybersecurity and privacy expectations can result in severe consequences. The **Privacy Act 1988** and the **Australian Privacy Principles (APPs)** mandate that institutions handling children's data do so lawfully, securely, and transparently (Office of the Australian Information Commissioner 2025). For a provider dealing with sensitive data—such as behavioural records, academic performance, and health information—non-compliance with these principles can attract civil penalties and trigger investigations.

In addition to privacy obligations, SafeStart is also governed by **the Child Safe Standards**, which require organisations working with minors to adopt systems that minimise risks across all operational domains, including digital safety (Commission for Children and Young People n.d.). This includes clear protocols for acceptable device use, content filtering, staff training, and incident response preparedness. These standards reinforce a duty of care that extends into cyberspace, framing cybersecurity as a component of overall child protection.

Further, **the eSafety Commissioner's guidelines** recommend essential digital safety measures for schools—such as implementing parental controls, teaching cyber hygiene, and deploying age-appropriate content filters (eSafety Commissioner 2025). Although these guidelines are not statutory law, they are increasingly treated as the expected minimum by regulators, parents, and accreditation bodies.

Legal and Financial Risk Exposure

Failure to act on these obligations exposes SafeStart Learning to both **legal claims and financial harm**. If a cybersecurity incident results in the loss of student data or online exploitation, families may lodge privacy complaints or pursue litigation—especially if it is found that the school lacked adequate preventive controls (Witzleb & Paterson 2020). Legal exposure includes breaches under the Privacy Act, negligence under civil law, and even potential criminal investigations in severe cases.

Financially, the implications go beyond legal fees. Response costs can include forensic investigation, system upgrades, third-party consulting, and compensation for affected families. Disruption to operations is also likely, as staff and leadership divert resources toward incident resolution. According to cybersecurity firm Gridware, the **average cost of a breach in the Australian education sector exceeds $3.7 million**, when accounting for both direct and indirect costs (Gridware n.d.).

Reputation, Enrolment, and Parental Trust

Perhaps the most critical risk is reputational. Parents view digital safety as a core part of their child's wellbeing. News of a breach involving student data or harm caused by online exposure

can spread quickly, damaging enrolment, stakeholder confidence, and institutional standing (Grande, Pore & Elesio 2025).

Reputational harm is amplified in the digital age, where parents may share concerns across social media or through online reviews. Once public trust is lost, recovery can take years—even with improved systems in place. Research shows that schools that experience cyber incidents face **long-term enrolment declines and increased oversight** from regulators and the community (Waller 2017).

On the other hand, schools that actively implement visible and effective cybersecurity frameworks—such as appointing a **Cyber Safety Officer**, conducting digital literacy workshops, and publishing annual cyber risk reports—are seen as responsible, modern, and trustworthy (Australian Institute of Company Directors 2024). These proactive steps not only mitigate risk but enhance SafeStart's value proposition in a competitive education market.

Recommended Cybersecurity Measures

Secure Student Devices and BYOD Policy

SafeStart Learning should either issue secured, centrally managed student devices or implement a strictly controlled BYOD policy. Centrally managed devices allow IT staff to configure security settings, install antivirus software, restrict app access, and remotely wipe devices if lost or compromised. This reduces the risk of malware infections or unauthorised data collection by third-party apps (Australian Cyber Security Centre 2024).

If BYOD is unavoidable, then SafeStart must enforce strict minimum requirements, including:

- Mandatory device registration and endpoint protection.
- Access via secure school VPN.
- Usage agreements signed by parents and students.

By controlling device security, the organisation minimises attack surfaces and aligns with **Child Safe Standards requiring** proactive risk reduction (Commission for Children and Young People n.d.).

Wi-Fi Security and Content Filtering

A robust school Wi-Fi system is essential for maintaining safe digital access. SafeStart should upgrade its infrastructure to enterprise-grade Wi-Fi with:

- **WPA3 encryption**
- **Network segmentation** (separating student, staff, and guest networks)
- **MAC address whitelisting** for connected devices.

Equally important is implementing **real-time content filtering**. Filters should be configured to block access to websites and services known to contain violent, explicit, or manipulative material (eSafety Commissioner 2025). Filters can be managed via cloud platforms or locally hosted systems and must be regularly updated to reflect evolving threats.

Failing to implement this measure exposes students to inappropriate content and violates legal duties outlined under the Privacy Act and Child Safe Standards (Office of the Australian Information Commissioner 2025).

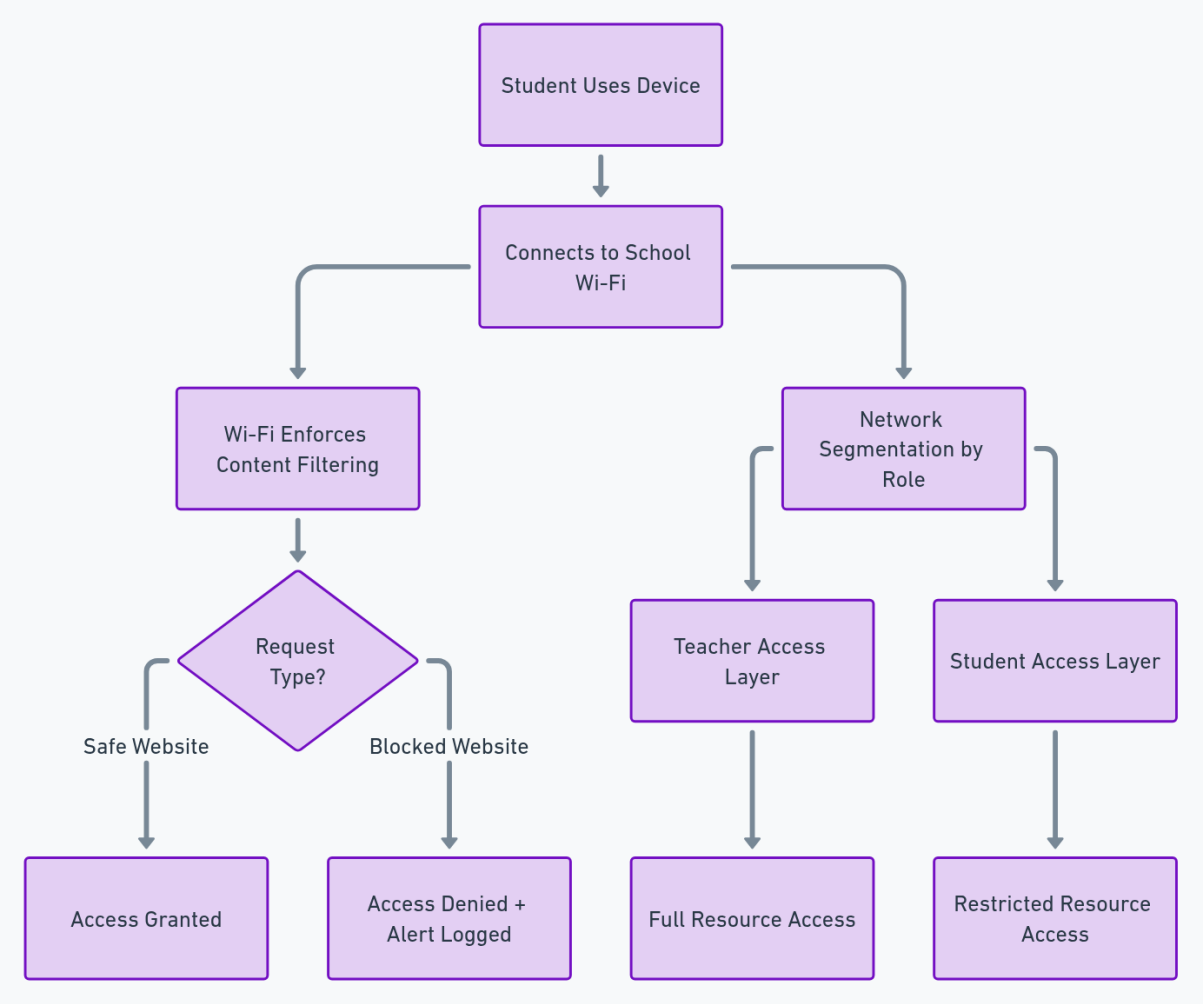


Figure 1: SafeStart Wi-Fi Network content filtering process using access control and segmentation.

Cyber Safety Education for Students, Staff, and Parents

Technology alone is insufficient, cybersecurity must be understood and practiced. SafeStart should roll out an age-appropriate **digital literacy curriculum** that teaches students how to:

- Recognise online scams and phishing.
- Report cyberbullying.
- Avoid oversharing personal information.

For teachers and administrators, regular workshops should cover safe online practices, reporting protocols, and privacy compliance (Tomczyk 2019). Parent-focused webinars or newsletters can extend this safety net into the home environment.

Studies show that when cybersecurity education is embedded in school culture, both incident frequency and severity decline (UNICEF 2012). These programs also satisfy **Child Safe Standards** requiring education about safety in all domains, including digital.

Cybersecurity Monitoring and Response Systems

SafeStart should adopt active monitoring tools to detect and alert staff to potential threats. These may include:

- **Keyword monitoring** on student chats and platforms for bullying or concerning words or terms.
- **Anomaly detection** systems that flag unusual access or data movement.
- **Maintain access logs** for all student and staff accounts for further investigations.

The school should also deploy endpoint protection software and intrusion detection systems (IDS) that alert IT staff to unauthorised access or policy violations (Australian Cyber Security Centre 2024).

Monitoring is especially critical in early detection of grooming and cyberbullying, which often go unnoticed until after harm occurs. These tools create a digital safety net, supporting staff in real-time threat response.

Incident Reporting Framework

SafeStart must adopt a formal **incident response plan** that outlines how cybersecurity events are reported, investigated, and escalated. This should include:

- Clear reporting lines for students and staff.
- Response timelines and communication responsibilities.
- Templates for notifying parents, regulators, and law enforcement if needed.

Regular testing of this framework (e.g., through tabletop exercises) ensures staff are prepared when real incidents occur. The existence of a codified plan also strengthens the school's ability to demonstrate compliance during audits (eSafety Commissioner 2025; Office of the Australian Information Commissioner 2025).

These combined technical and behavioural strategies not only reduce the likelihood of a cybersecurity breach but also show SafeStart Learning's commitment to digital child safety. Implementation of these recommendations will position the institution as a sector leader in online protection and reinforce stakeholder trust.

Governance and Oversight

Appointment of a Cyber Safety Officer

To ensure cybersecurity becomes an ongoing strategic priority, SafeStart Learning should appoint a **Cyber Safety Officer (CSO)**. This role would be responsible for:

- Overseeing the implementation of cybersecurity policies.
- Monitoring digital risks specific to child safety.
- Serving as a liaison between technical staff, school leadership, and parents.

The CSO should have both technical awareness and a strong understanding of the regulatory landscape, including the **Privacy Act**, **Child Safe Standards**, and recommendations from the **eSafety Commissioner** (eSafety Commissioner 2025; Office of the Australian Information Commissioner 2025). Their mandate should also include staying up to date with emerging threats and proposing timely updates to the school's digital safety protocols.

By assigning ownership of digital child safety, SafeStart aligns itself with best practices in educational governance and risk management (UNICEF 2017).

Formation of an Internal Cybersecurity Committee

In addition to appointing a CSO, SafeStart should establish an internal **Cybersecurity Governance Committee**. This multidisciplinary group would include:

- Senior leadership (Principal, Deputy Principals)
- The Cyber Safety Officer
- IT and teaching staff
- A parent or school board representative

The committee would meet quarterly to:

- Review security audit results.
- Track progress on cyber safety initiatives.
- Update digital policies in line with new threats or technologies.
- Review any incidents or near-misses and refine response strategies.

The committee serves as a formal accountability mechanism, ensuring cybersecurity remains a standing agenda item in strategic planning and board-level discussions (Commission for Children and Young People n.d.). It also fosters collaboration between technical, administrative, and community stakeholders, which is crucial in environments where children's wellbeing is at stake.

By embedding governance into its digital safety efforts, SafeStart ensures that its cybersecurity posture is not reactive but sustained, reviewed, and improved over time. These governance structures also demonstrate to regulators and parents that SafeStart takes its duty of care seriously and is committed to leadership in digital child protection (Australian Cyber Security Centre 2024).

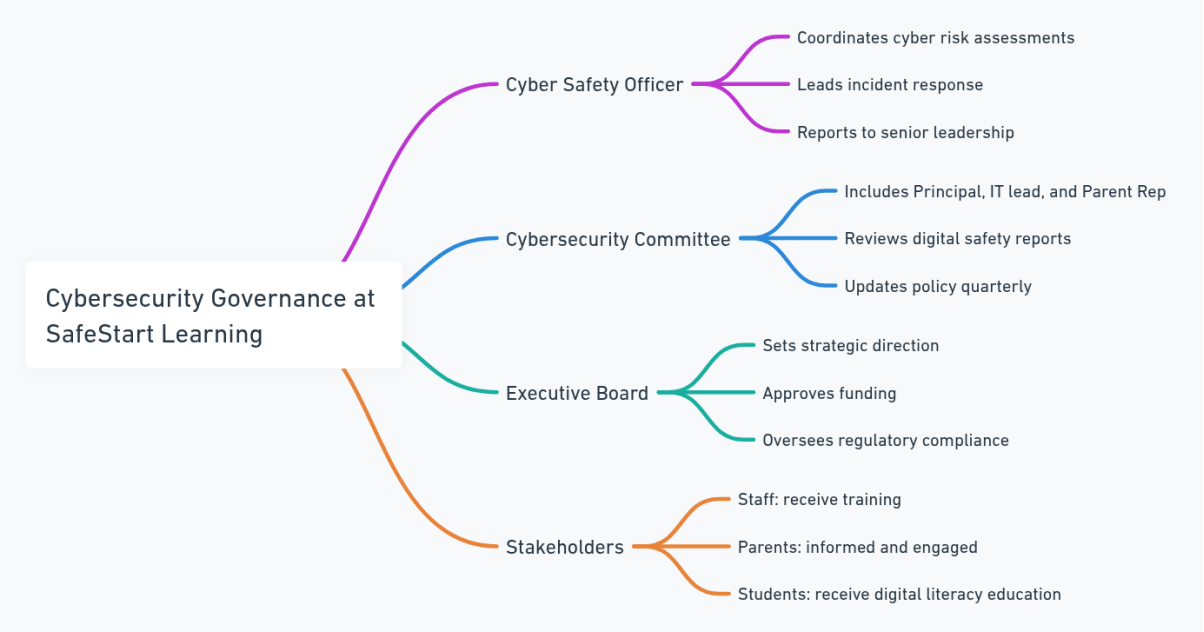


Figure 2: Proposed cybersecurity governance model for SafeStart Learning.

Case Examples and Impact Scenarios

Real-world Breach Examples Involving Children

Case 1: Catholic Education South Australia (CESA) Data Breach, 2023

In mid-2023, a cyber-attack on Catholic Education South Australia (CESA) compromised student records across multiple schools. The attackers gained unauthorised access to sensitive data, including names, addresses, and academic information. Although no financial data was stolen, the breach triggered significant media scrutiny, an internal investigation, and a sharp drop in parent confidence (UNICEF 2017).

The incident exposed gaps in the organisation's incident detection and data governance mechanisms. CESA had not implemented adequate endpoint monitoring tools or multi-factor authentication on staff portals, which allowed threat actors to move laterally within systems undetected. This case underscores the need for real-time threat monitoring and access control in educational environments.

Case 2: Student Harassment via Messaging Platform in Victoria, 2022

A Year 5 student in a Victorian school was targeted with threatening messages via a school-endorsed chat platform. Despite teacher oversight, the abuse persisted for weeks before detection. The incident resulted in a formal complaint to the Victorian Department of Education and a full review of the platform's use in primary schools (Commission for Children and Young People n.d.).

This case highlights the dangers of assuming platforms are inherently safe and the importance of integrating **keyword monitoring**, staff training, and clear escalation procedures.

Model Practices from Comparable Organisations

Best Practice: NSW Department of Education's Cyber Safety Strategy (2024)
The NSW Department of Education implemented a comprehensive cyber safety strategy in 2024 that includes:

- Organisation-managed student devices with endpoint protection.
- A centralised incident reporting tool accessible by staff, students, and parents.
- Regular cyber safety education embedded into the digital curriculum.
- Quarterly digital audits conducted by a cybersecurity governance panel (Australian Cyber Security Centre 2024).

This initiative has led to a measurable reduction in reported incidents and received national recognition from the **eSafety Commissioner**. It serves as a model for how a school system can proactively address digital risks while aligning with regulatory standards.

Best Practice: eSafety Commissioner – Toolkit for Schools
Developed by the Australian Government, the toolkit aimed as schools focuses on:

- Prepare the school
- Engage with the community
- Educate student, staff and parents
- Respond to incidents (eSafety Commissioner 2024)

SafeStart Learning can draw from these standards to build a relevant, informed cybersecurity framework and policies.

These examples demonstrate that cyber incidents involving children are not hypothetical—they are frequent, underreported, and highly damaging. Institutions that implement structured policies, education programs, and oversight mechanisms are far better positioned to protect children and retain stakeholder trust.

Implementation Strategy

Phased Rollout and Budget Considerations

Implementing robust cybersecurity for children requires a structured, phased approach to ensure continuity, compliance, and cost-efficiency. SafeStart Learning can adopt a **three-phase rollout** across 12 months:

Phase 1 – Immediate (0–3 months): Policy and Infrastructure

- Deploy content filtering tools and WPA3 Wi-Fi encryption across all campuses.
- Begin issuing school-managed devices for high-risk age groups or enforce BYOD controls.
- Assign an interim Cyber Safety Officer from existing IT or compliance staff.
- Estimated budget: AUD $25,000 for infrastructure upgrades, licensing, and training setup.

Phase 2 – Mid-Term (4–8 months): Governance and Education

- Formalise the Cybersecurity Governance Committee.
- Begin cyber safety training for staff and introductory sessions for parents.
- Launch a digital literacy curriculum for students, focusing on safe browsing, password hygiene, and reporting abuse.
- Estimated budget: AUD $10,000 for educational resources, materials, and committee operations.

Phase 3 – Long-Term (9–12 months): Monitoring and Incident Response

- Implement monitoring tools for student platforms (e.g., keyword alerts).
- Finalise and test a formal incident response framework.
- Conduct quarterly security audits and board-level risk reviews.
- Estimated budget: AUD $15,000 for monitoring software, risk assessment, and audit support.

Costs should be included in SafeStart's annual strategic budget under risk management and child safety compliance. Where possible, partnerships with vendors or government-supported cyber programs may reduce cost burdens.

Staff Training and Policy Updates

Cybersecurity is not solely a technical upgrade—it requires cultural change. All SafeStart staff must receive:

- Annual cybersecurity awareness training, including real-world case studies.
- A briefing on updated school policies regarding acceptable digital use, reporting lines, and data handling.
- Access to secure reporting channels for suspected incidents or risks.

In parallel, parents will receive newsletters and optional online sessions covering child-safe apps, social media risks, and the school's digital safety expectations.

School-wide policy updates—including privacy, acceptable use, and BYOD—must be revised and communicated transparently. These policies should be co-signed by parents as part of enrolment or device issuance procedures.

This strategic rollout ensures SafeStart Learning balances **child protection**, **regulatory compliance**, and **practical resourcing**—while fostering a digitally safe learning environment from the ground up.

Conclusion

Digital safety is now an essential pillar of student wellbeing. For SafeStart Learning, the need to address cybersecurity risks facing children is both urgent and strategic. The risks—ranging from data breaches and cyberbullying to online grooming and exposure to harmful content—can have long-lasting consequences for students, families, and the institution alike.

This paper demonstrates cybersecurity is not merely an IT issue but a **core governance concern**. Institutions that ignore it face not only technical vulnerabilities but also legal liability, regulatory breaches, and reputational harm. Conversely, organisations that take a proactive, whole-of-school approach to digital child protection can build deeper trust with parents, staff, and the broader community.

The recommendations provided include secure device management, content filtering, cyber literacy programs, monitoring tools, and board-level oversight—are not only feasible but aligned with best practices across the education sector.

Now is the time for SafeStart Learning's Board to act. By implementing these strategies, the organisation can lead by example, safeguard its students, and build a resilient, future-ready digital environment for learning.

References

Australian Institute of Company Directors (AICD) 2024, *Cyber security governance principles*, Australian Institute of Company Directors, viewed 30 May 2025, https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-tools/board/cyber-security-governance-principles-web3.pdf.

Australian Cyber Security Centre 2024, *Protect your children online: A guide to cyber security for parents and carers*, Australian Government, viewed 27 March 2025, https://www.cyber.gov.au/protect-yourself/staying-secure-online/protecting-your-family/protect-your-children-online.

Commission for Children and Young People n.d., *Raising concerns about child safety*, Child Safe Standards, viewed 30 April 2025, https://ccyp.vic.gov.au/child-safe-standards/raising-child-safety-matters/.

Department of Education 2025, *Digital technologies – responsible use*, Victorian Government, viewed 1 June 2025, https://www2.education.vic.gov.au/pal/digital-technologies-responsible-use/policy.

eSafety Commissioner 2024, *Toolkit for schools*, viewed 27 March 2025, https://www.esafety.gov.au/educators/toolkit-schools.

eSafety Commissioner 2025, *Parental controls: How to keep your child safe*, Australian Government, viewed 27 March 2025, https://www.esafety.gov.au/parents/issues-and-advice/parental-controls.

Grande, HR, Pore, NO & Elesio, JM 2025, 'The impact of social media hacking incidents on school reputation: An in-depth investigation of crisis response strategies', *International Journal of Research and Innovation in Applied Science*, vol. 10, no. 1, pp. 118–135.

Gridware n.d., *Cybersecurity for the education industry*, viewed 20 April 2025, https://www.gridware.com.au/industry/cybersecurity-for-education/.

Holloway, D, Green, L & Livingstone, S 2013, *Zero to eight: Young children and their internet use*, EU Kids Online, London School of Economics and Political Science, London.

Office of the Australian Information Commissioner 2023, *Children's privacy and data protection*, Australian Government, viewed 27 March 2025, https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/children-and-young-people.

Palfrey, J & Gasser, U 2011, *Born digital: Understanding the first generation of digital natives*, Basic Books, New York.

Privacy Act 1988 (Cth).

Shen, L, Chen, I & Su, A 2017, ‘Cybersecurity and data breaches at schools’, in *Cybersecurity breaches and issues surrounding online threat protection*, IGI Global, pp. 144–174.

Tomczyk, L 2019, ‘Digital literacy in the area of e-safety among teachers (Second stage of the primary school) in Poland’, in *Conference proceedings of eLearning and Software for Education (eLSE)*, vol. 15, no. 2, pp. 130–135.

Waller, M 2017, ‘The role of schools in children's online safety’, in *Online risk to children: Impact, protection and prevention*, pp. 217–230.

Witzleb, N & Paterson, M 2020, *Privacy risks and harms for children and other vulnerable groups in the online environment*, Monash University.

Whittle, H, Hamilton-Giachritsis, C, Beech, A & Collings, G 2013, ‘A review of online grooming: Characteristics and concerns’, *Aggression and Violent Behavior*, vol. 18, no. 1, pp. 62–70.

Wold, T, Aristodemou, E, Dunkels, E & Laouris, Y 2009, ‘Inappropriate content’, in Livingstone, S & Haddon, L (eds), *Kids online: Opportunities and risks for children*, Bristol University Press, pp. 135–146.

UNICEF 2012, *Child online safety: Global challenges and strategies*, viewed 27 March 2025, https://www.unicef.org/media/66821/file/Child-Safety-Online.pdf.

UNICEF 2017, *Children in a digital world*, viewed 27 March 2025, https://www.unicef.org/media/48581/file/SOWC_2017_ENG.pdf.

Zhao, J, Wang, G, Dally, C, Slovak, P, Edbrooke-Childs, J, Van Kleek, M & Shadbolt, N 2019, ‘"May I make up a silly name?” Understanding children's perception of privacy risks online’, in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1–13.

Appendix A – Team Roles & Responsibilities

Week	Date	Key Activities	Phranavh Sivaraman	Simon Wilson
4	27 Mar	Topic selection and initial planning	Participated in topic brainstorming and meeting discussions	Participated in topic brainstorming and meeting discussions
5	03 Apr	Research on cybersecurity risks	Conducted research on online safety, cyberbullying, and school-specific risks	Conducted research on data privacy, legal frameworks, and children's rights
6	10 Apr	Strategy refinement and scope definition	Collaborated on defining focus (SafeStart Learning); aligned it with regulations	Contributed ideas and confirmed direction during meeting discussions
7	17 Apr	Drafting proposal outline (Task 3B)	Collaboratively drafted the 400-word introduction and structure	Collaboratively drafted the 400-word introduction and structure
8	24 Apr	Literature review and case study research	Researched Australian breach examples and real-world implications	Researched model practices and international guidelines (eSafety Comm., NSW DoE)
9	01 May	Section writing and refinement	Contributed equally to drafting Sections 2–4	Contributed equally to drafting Sections 5–6
10	08 May	Visuals and diagram creation	Created draft diagrams in Whimsical; refined flowcharts and mindmaps	Reviewed visual structure, captions, and suggested revisions
11	15 May	Case examples and scenario planning	Co-developed Section 7 on real-world examples	Co-developed Section 7 on real-world examples
12	22 May	Full draft integration and editing	Edited overall structure, ensured logical flow between sections	Edited overall structure, checked grammar, tone, and coherence
13	03 Jun	Proofreading, referencing, and submission	Finalised referencing and formatting; uploaded submission on Canvas	Cross-checked in-text citations and provided final review feedback

Appendix B – Task Allocation Table

Task Description	Assigned Members	Date Assigned	Status	Date Completed
Topic brainstorming and selection	Phranavh & Simon	27 Mar 2025	Completed	28 Mar 2025
Initial research on online threats to children	Phranavh & Simon	01 Apr 2025	Completed	03 Apr 2025
Review of Australian privacy and child safety laws	Phranavh & Simon	04 Apr 2025	Completed	06 Apr 2025
Drafting the proposal and introduction outline (Task 3B)	Phranavh & Simon	07 Apr 2025	Completed	10 Apr 2025
Case study and impact research (CESA breach, VIC incident)	Phranavh & Simon	12 Apr 2025	Completed	17 Apr 2025
Writing Sections 2–4 (Threats, Context, Business Risk)	Phranavh & Simon	18 Apr 2025	Completed	24 Apr 2025
Writing Sections 5–6 (Recommendations, Governance)	Phranavh & Simon	25 Apr 2025	Completed	01 May 2025
Creation of diagrams and visual assets (Whimsical)	Phranavh & Simon	02 May 2025	Completed	04 May 2025
Drafting Section 7 (Case Examples and Best Practices)	Phranavh & Simon	05 May 2025	Completed	09 May 2025
Writing Section 8 (Implementation Strategy)	Phranavh & Simon	10 May 2025	Completed	14 May 2025
Finalising Section 9 (Conclusion) and proofreading	Phranavh & Simon	15 May 2025	Completed	22 May 2025
Compiling References (RMIT Harvard)	Phranavh & Simon	29 May 2025	Completed	01 Jun 2025
Final proofreading, appendix, and formatting	Phranavh & Simon	01 Jun 2025	Completed	03 Jun 2025
Submission on Canvas	Phranavh (on behalf of team)	03 Jun 2025	Completed	03 Jun 2025

Appendix C – Minutes of Meeting

Meeting Minutes

Date	**Thursday 27 March 2025**
Time	5:00 PM
Location	080.01.002
Team Members	
Phranavh Sivaraman	Attended
Simon Wilson	Attended
Items and Issues	Topic agreed: Cyber Security for Children Meeting time agreed: Thursday 5pm
Work for the following week	
Phranavh	Conduct Research on topic Draft proposal
Simon	Conduct Research on topic Draft proposal
Next Meeting	Thu 03 April, 5:00 PM @ 080.01.002

Meeting Minutes

Date	**Thursday 03 April 2025**
Time	5:00 PM
Location	080.01.002
Team Members	
Phranavh Sivaraman	Attended
Simon Wilson	Attended
Items and Issues	Discussed research
Work for the following week	
Phranavh	Research on Online Safety
Simon	Research on Data privacy
Next Meeting	Thu 10 April, 5:00 PM @ 080.01.002

Meeting Minutes

Date	**Thursday 10 April 2025**
Time	5:00 PM
Location	080.01.002
Team Members	
Phranavh Sivaraman	Attended
Simon Wilson	Attended
Items and Issues	Discussed topics and future direction
Work for the following week	
Phranavh	Consider business options for target of paper
Simon	Consider business options for target of paper
Next Meeting	Thu 17 April, 5:00 PM @ 080.01.002

Meeting Minutes

Date	**Thursday 17 April 2025**
Time	5:00 PM
Location	080.01.002
Team Members	
Phranavh Sivaraman	Attended
Simon Wilson	Attended
Items and Issues	Review feedback from Proposal. Refined concept for assessment
Work for the following week	
Phranavh	Draft proposal
Simon	Draft proposal
Next Meeting	Thu 24 April, 5:00 PM @ Online

Meeting Minutes

Date	**Thursday 24 April 2025**
Time	5:00 PM
Location	Online
Team Members	
Phranavh Sivaraman	Attended
Simon Wilson	Attended
Items and Issues	Review draft. Discuss topics
Work for the following week	
Phranavh	Review and edit proposal.
Simon	Review and edit proposal.
Next Meeting	Thu 01 May, 5:00 PM @ 080.01.002

Meeting Minutes

Date	**Thursday 01 May 2025**
Time	5:00 PM
Location	080.01.002
Team Members	
Phranavh Sivaraman	Attended
Simon Wilson	Attended
Items and Issues	Shared information on research conducted
Work for the following week	
Phranavh	Research and prepare for school based solutions
Simon	Research and prepare for school based issues
Next Meeting	Thu 08 May, 5:00 PM @ 080.01.002

Meeting Minutes

Date	**Thursday 08 May 2025**
Time	5:00 PM
Location	080.01.002
Team Members	
Phranavh Sivaraman	Attended
Simon Wilson	Attended
Items and Issues	Shared information on research conducted and discussed drafting of content
Work for the following week	
Phranavh	Draft assessment for school based solutions
Simon	Draft for school based issues
Next Meeting	Thu 15 May, 5:00 PM @ 080.01.002

Meeting Minutes

Date	**Thursday 15 May 2025**
Time	5:00 PM
Location	080.01.002
Team Members	
Phranavh Sivaraman	Attended
Simon Wilson	Attended
Items and Issues	Discussed issues around identifying existing supporting literature
Work for the following week	
Phranavh	Look at differing sources of information
Simon	Look at differing sources of information
Next Meeting	Thu 22 May, 5:00 PM @ 080.01.002

Meeting Minutes

Date	**Thursday 22 May 2025**
Time	5:00 PM
Location	080.01.002
Team Members	
Phranavh Sivaraman	Attended
Simon Wilson	Attended
Items and Issues	Discuss progress
Work for the following week	
Phranavh	No expectations for the next week due to completing assignments
Simon	No expectations for the next week due to completing assignments
Next Meeting	Thu 29 May, 5:00 PM @ 080.01.002

Meeting Minutes

Date	**Thursday 29 May 2025**
Time	5:00 PM
Location	080.01.002
Team Members	
Phranavh Sivaraman	Attended
Simon Wilson	Attended
Items and Issues	Discuss progress and next steps to finalise
Work for the following week	
Phranavh	Need to review each others work and provide feedback
Simon	Need to review each others work and provide feedback
Next Meeting	Tue 03 June, 8:00 PM @ 080.04.006

Meeting Minutes

Date	**Tuesday 03 June 2025**
Time	8:00 PM
Location	080.04.006
Team Members	
Phranavh Sivaraman	Attended
Simon Wilson	Attended
Items and Issues	Discuss current draft
Work for the following week	
Phranavh	Proof read, and review referencing style
Simon	Proof read, and review referencing style
Next Meeting	Nil, calls as required.

Appendix D – Challenges Faced and How We Overcame Them

Throughout the 10-week duration of this project, our team encountered a range of academic, technical, and collaborative challenges. Each obstacle pushed us to adapt, rethink our approach, and develop stronger project management and research strategies. The challenges are outlined below in chronological order, along with the detailed solutions we implemented.

1. Narrowing the Topic Scope to a Researchable, Impactful Theme (Week 4–5)

Challenge:
Our initial discussions focused on broad areas like "Cybersecurity in Schools" and "Children's Online Safety." However, these themes encompassed too many sub-topics (cyberbullying, ransomware, surveillance, app privacy, etc.) and lacked a clearly defined end-user. This risked making our paper vague and unfocused.

Resolution:
After extensive brainstorming, we reframed the topic around a **specific educational institution**, *SafeStart Learning*, a fictional but realistic early childhood education provider. This allowed us to contextualise our research within an actionable and relatable setting. It also aligned well with real-world board-level risk assessments. We mapped regulatory frameworks like the **Child Safe Standards** and the **Privacy Act 1988** to this setting, giving our work a practical application.

This clarity of scope helped shape our literature review, risk identification, and recommendations, making the entire paper more targeted and professional.

2. Limited Availability of Australian centric academic sources (Week 5–6)

Challenge:
We initially relied heavily on scholarly databases such as Google Scholar and ProQuest. However, we quickly realised that academic papers on children's digital privacy in Australian primary education contexts were sparse. Most existing work was international or focused on older students (high school/university). This created a risk that our paper might not meet local regulatory or policy expectations.

Resolution:
We adapted by expanding our research strategy. We included **grey literature** such as:

- Government white papers
- Regulatory websites (eSafety Commissioner, OAIC)
- Reports by non-profit bodies like UNICEF
- Practitioner guides (e.g., ACSC's "Protect Your Children Online")

In total, we referenced 21 diverse sources, including **peer-reviewed articles**, **government frameworks**, and **policy briefs**. This blended approach allowed us to address both conceptual and operational aspects of cybersecurity in an Australian early learning context.

3. Designing a Legal and Governance Framework Without Legal Expertise (Week 6–7)

Challenge:
Interpreting the **Privacy Act 1988**, **Australian Privacy Principles**, and **Child Safe Standards** was initially overwhelming. We lacked formal training in legal interpretation and found some clauses difficult to translate into practical, school-level actions.

Resolution:
Simon focused on extracting the most relevant sections by referencing secondary summaries from the Office of the Australian Information Commissioner (OAIC), which included simplified language. We mapped these legal obligations to specific school activities such as data collection, device issuance, and incident reporting. We also cited real-world data breach case studies (e.g., CESA breach) to show non-compliance consequences. This helped us convert abstract regulations into concrete governance recommendations such as the appointment of a **Cyber Safety Officer** and formation of a **Cybersecurity Governance Committee**.

4. Collaborative Writing and Maintaining Tone Consistency (Week 7–10)

Challenge:
Writing collaboratively in shared documents occasionally led to inconsistencies in tone, use of technical language, and formatting. For example, some sections were overly technical, while others leaned toward informal or explanatory language. Without a unified tone, the paper risked appearing disjointed.

Resolution:
We conducted joint reviews every 1–2 weeks, during which we edited each other's drafts. We agreed on a tone guideline: professional, but understandable to a non-technical executive reader. Phranavh also created a style template, applying consistent heading levels, citation formats, and font usage. Simon edited for flow and clarity, especially in areas like the Executive Summary and Implementation Strategy. This revision process made our final paper coherent and polished.

5. Visual Communication and Custom Diagram Design (Week 8–10)

Challenge:
We wanted to go beyond stock diagrams and design original visual aids that would effectively communicate complex topics (e.g., Wi-Fi network segmentation, cybersecurity governance model). However, visual design was time-consuming and required extra software like Whimsical.

Resolution:
Phranavh led the design process, starting with flowcharts in Whimsical and later converting them into Word-compatible images. Simon assisted in refining these visuals with accurate captions and annotations. We also tested each diagram with peers to ensure clarity. Including these original visuals helped fulfil the rubric's requirement for mixed communication styles and gave our report a professional edge.

6. Managing Workload During High-Pressure Weeks (Week 9–11)

Challenge:
During this period, we were simultaneously working on assignments in other units like **COSC2737** and **INTE2655**, which included technical labs, threat modelling, and video assessments. This affected our ability to consistently meet as a team and delayed writing progress for Sections 6 to 8.

Resolution:
We restructured our work into **asynchronous modules**. For example:

- One member drafted while the other reviewed.
- We worked in 3-hour bursts instead of daily sprints.
- We prioritised section completion by deadline impact (Executive Summary > Recommendations > Case Examples).

We also agreed to extend final editing and referencing into Week 13 to ensure quality. This reallocation of time and energy kept our project on track while managing academic burnout.

7. Evidence of Individual Contribution and Shared Ownership

Challenge:
As the scope expanded, there was a risk of unintentionally drifting into isolated tasks, which could reduce the effectiveness of collaboration.

Resolution:
We formalised our contributions as follows:

- **Phranavh**: Lead designer, strategist for content filtering, infrastructure upgrades, and implementation plan. He also managed version control and final formatting in Word.
- **Simon**: Lead researcher for legal, governance, and policy areas. He drafted the majority of the "Business and Legal Implications" and "Governance" sections.
- Both: Co-authored the Executive Summary, Background, and Case Studies. Jointly reviewed citations and grammar.

This ensured equal contribution and built trust in shared responsibility.

8. Final Editing, Proofreading, and Compliance Checks (Week 13)

Challenge:
The final document needed strict compliance with:

- RMIT Harvard referencing style
- Auto-generated Table of Contents
- Word limit under 3,500 words
- Academic formatting (12pt Times New Roman, single spacing)

Any errors in these areas could impact our final grade.

Resolution:
We cross-checked formatting against previous assignments and RMIT Library guides. We verified that all 8 sources were cited both inline and in the reference list. Phranavh built the auto TOC, and Simon validated the flow using the rubric criteria. The last 48 hours before submission were fully devoted to proofreading and formatting—without content changes—to ensure perfect compliance.

Conclusion

Despite encountering multiple challenges—including topic ambiguity, source scarcity, legal interpretation, and intense time pressure—our team responded with initiative, planning, and a shared growth mindset. We applied agile techniques to coordinate our efforts, developed original insights rooted in real-world policy frameworks, and created a submission that addresses cybersecurity not just as a technical issue, but as a holistic risk management challenge for education providers.

This project has strengthened our abilities in:

- Applied cybersecurity governance
- Strategic technical communication
- Executive-level risk reporting
- Cross-functional team collaboration

Appendix E – Team-Level and Individual Contributions Table

Week	Date	Key Activities and Contributions (Team)
Week 4	27 Mar 2025	Brainstormed cybersecurity topics relevant to children. Agreed on focusing on "Cyber Security for Children" and selected *SafeStart Learning* as a realistic institutional case. Discussed executive readability, relevance to school settings, and board-level concerns.
Week 5	3 Apr 2025	Drafted the project proposal with a 100-word outline, team contract, and semester plan. Divided research tasks: Simon focused on the Privacy Act 1988 and child protection laws; Phranavh explored early learning vulnerabilities and emerging threats like gamified phishing and BYOD risks.
Week 6	10 Apr 2025	Conducted deeper research. Identified gaps in scholarly literature and shifted toward grey literature (eSafety, UNICEF, OAIC). Narrowed scope to school-level interventions. Decided to map threats to specific legal duties and governance structures in SafeStart Learning.
Week 7	17 Apr 2025	Drafted Task 3B discussion paper outline. Defined major sections: Executive Summary, Threat Landscape, Business & Legal Risks, Recommendations, Governance, Case Studies, Implementation Strategy, and Conclusion. Planned to use real-world incidents and regulatory references.
Week 8	24 Apr 2025	Continued literature review and drafted Sections 2–4. Simon researched legal obligations; Phranavh reviewed online safety stats and reports. Identified two case studies: CESA breach (2023) and a Year 5 student harassment case in Victoria. These were used to illustrate real-world risks.
Week 9	1 May 2025	Jointly drafted threat landscape and legal risks sections. Mapped data privacy, cyberbullying, grooming, and scams to school-level responsibilities under the Child Safe Standards and Australian Privacy Principles (APPs). Discussed ethical responsibilities and potential operational consequences.
Week 10	8 May 2025	Developed original diagrams: Wi-Fi filtering and governance models. Phranavh designed visual drafts; Simon edited structure and explanatory captions. Co-wrote the "Recommended Measures" section—covering device control, content filtering, and education for students, staff, and families.
Week 11	15 May 2025	Reviewed visuals and refined recommendations. Integrated real-time monitoring, incident response frameworks, and keyword detection ideas into the plan. Planned governance strategies like appointing a Cyber Safety Officer and forming a cybersecurity committee.
Week 12	22 May 2025	Began integrating all sections into one cohesive document. Ensured logical progression from risk to solution. Aligned content to address

Week	Date	Key Activities and Contributions (Team)
		board-level concerns—highlighting institutional accountability, parental trust, and regulatory compliance. Reviewed all section headings and transitions.
Week 13	3 Jun 2025	Final proofreading, formatting, and referencing in RMIT Harvard style. Inserted automatic Table of Contents. Verified inline citations, polished grammar and tone, cross-checked all appendices. Phranavh led formatting and reference integrity; Simon focused on clarity and logical flow. Uploaded final file to Canvas.

Contribution

Team Member	Contribution Area	Detailed Contributions
Phranavh Sivaraman	**Research & Technical Insight**	Researched emerging cyber threats specific to early childhood users such as gamified phishing, unsafe educational apps, and misconfigured school Wi-Fi networks. Brought forward UNICEF policy briefs and incorporated risk psychology of young learners.
Phranavh Sivaraman	**Threat Landscape & Implementation Strategy**	Took primary responsibility for drafting the "Cybersecurity Threat Landscape" and "Implementation Strategy" sections. Focused on mapping specific threats (grooming, scams, cyberbullying) to realistic school-level countermeasures. Outlined a 3-phase cybersecurity implementation plan (Immediate, Mid-Term, Long-Term).
Phranavh Sivaraman	**Visual Diagrams & Communication Aids**	Created original diagrams using Whimsical including: • SafeStart Wi-Fi Content Filtering Flow • Cybersecurity Governance Structure • Incident Reporting Framework Converted diagrams for Word format and ensured they were accessible, explanatory, and aligned to adjacent content.
Phranavh Sivaraman	**Technical Recommendations**	Proposed secure BYOD protocols, WPA3 enterprise-grade Wi-Fi encryption, device segmentation, VPN use, and endpoint protection tools. Suggested age-appropriate cyber literacy programs and keyword monitoring systems for bullying/grooming detection.
Phranavh Sivaraman	**Formatting & Referencing**	Led document formatting: applied heading styles for auto TOC, cleaned up spacing, ensured compliance with 12pt Times New Roman, and applied consistent margins.

Team Member	Contribution Area	Detailed Contributions
		Managed RMIT Harvard referencing throughout — cross-checked inline citations and formatted 8 sources meticulously.
Phranavh Sivaraman	**Review & Editing**	Conducted the final full-document proofreading pass for grammar, flow, clarity, and tone consistency. Polished the Executive Summary and Conclusion to align with board-level communication expectations. Created backup copies and final Canvas upload.
Phranavh Sivaraman	**Project Management**	Maintained document version control using shared Google Docs and OneDrive. Recorded progress in each meeting, tracked team's weekly goals, and ensured alignment to semester plan. Suggested timeline extensions where necessary to preserve quality without missing deadlines.
Simon Wilson	Legal and Policy Research	Focused extensively on reviewing the Privacy Act 1988, Australian Privacy Principles, Child Safe Standards, and eSafety frameworks. Identified practical implications for educational institutions that fail to comply. Interpreted regulatory expectations and converted them into actionable school policies.
Simon Wilson	Business and Legal Implications Section	Took lead on writing Sections 4–5 of the paper. Mapped legal obligations to SafeStart Learning's institutional structure. Evaluated risk scenarios such as data breaches and reputational damage. Included statistics on average costs of breaches in education.
Simon Wilson	Cybersecurity Governance Recommendations	Proposed appointing a Cyber Safety Officer, forming a Cybersecurity Governance Committee, and implementing school-wide auditing and risk review procedures. Mapped these roles against real-world best practices from the NSW Department of Education and eSafety Commissioner's toolkit.
Simon Wilson	Case Studies and Examples	Researched and drafted the section on real-world incidents including: • 2023 Catholic Education South Australia (CESA) breach • Year 5 chat platform cyberbullying case in Victoria

Team Member	Contribution Area	Detailed Contributions
		Added analysis on how these events could have been mitigated with proper governance.
Simon Wilson	Language and Structure Review	Reviewed each section for tone consistency and clarity. Ensured the writing was appropriate for a board-level audience, with minimal technical jargon. Reworked paragraph transitions, especially in the Governance and Recommendations sections.
Simon Wilson	Joint Section Development	Co-authored the Executive Summary, Background and Context, and Conclusion with Phranavh. Jointly aligned each section to rubric categories like Risks, Governance, and Strategic Response. Rewrote paragraphs for impact and brevity where needed.
Simon Wilson	Peer Review and Collaboration	Frequently reviewed Phranavh's drafts and provided critical feedback on structure, technical clarity, and diagram alignment. Maintained meeting agendas, and proactively suggested edits in shared docs. Collaborated on citations and caption text for visuals.

Appendix F – Team Learning Reflection

Throughout the course of this project, our team has undergone a profound journey of academic, technical, and personal growth. While the original goal was to deliver a high-quality discussion paper addressing "Cyber Security for Children," the experience ultimately became a transformative learning opportunity that deepened our understanding of cybersecurity governance, policy integration, real-world risk modelling, and collaborative project execution in a professional context.

At the outset, our understanding of cybersecurity was largely focused on network threats, malware, and data protection tools. However, through intensive research, analysis, and discussions, we came to appreciate that cybersecurity in educational settings is much broader. It intersects with regulatory compliance, behavioural psychology, ethical responsibility, and institutional governance. By grounding our work within the fictional but plausible setting of *SafeStart Learning*, we were able to apply abstract principles in a realistic context—something that enhanced both our critical thinking and problem-solving capabilities.

One of the most valuable takeaways from this project was the realisation that cybersecurity is not just about tools, it's about people, policy, and proactive culture. We learned how to align technical solutions like endpoint protection and keyword monitoring with legal requirements like the Privacy Act 1988 and the Child Safe Standards. This taught us the importance of translating legislation into actionable steps for an organisation—a skill that will be crucial in any future GRC or cybersecurity advisory role we take on.

Our team also gained practical insights into executive-level communication. Crafting a discussion paper aimed at a Board of Directors required us to shift our tone, simplify jargon, and present risks and recommendations in a way that was concise, persuasive, and strategic. This exercise significantly improved our professional writing and taught us how to communicate complex concepts to non-technical stakeholders.

The research process itself was eye-opening. We had to expand beyond traditional scholarly articles and dive into government publications, regulatory guidelines, and tools like eSafety Commissioners' Toolkit for Schools. This exposed us to interdisciplinary research practices and highlighted the value of grey literature in policy-oriented work. By combining Australian government reports, international best practices, and real-world case studies, we built a multidimensional understanding of the issue.

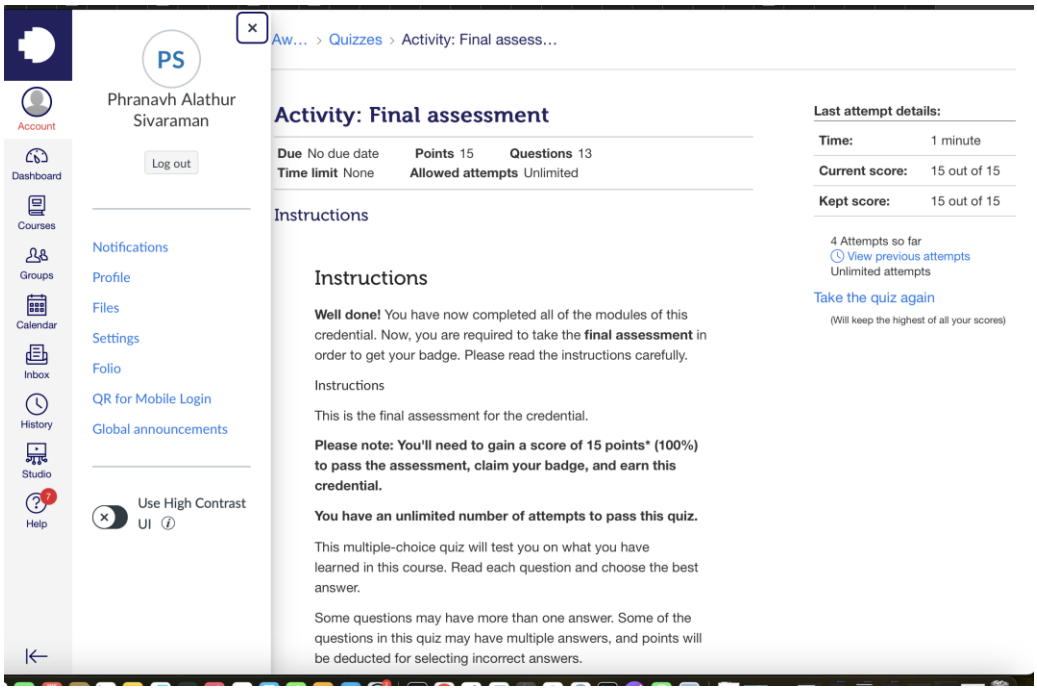
Collaboratively, we improved our project management and peer feedback skills. Using agile-inspired weekly sprints, we maintained a consistent workflow despite competing academic demands. Document version control, weekly stand-ups, and shared editing responsibilities ensured accountability and transparency. Most importantly, we developed mutual respect for each other's strengths—Phranavh's strategic thinking and technical structuring, and Simon's legal fluency and governance insight.

This project also instilled in us a deeper sense of ethical responsibility. As future cybersecurity professionals, we now understand that protecting children online is not just a compliance requirement—it's a moral imperative. The risks children face today are evolving rapidly, and institutions must act not only to prevent harm but to foster digitally safe environments where children can learn, grow, and thrive.

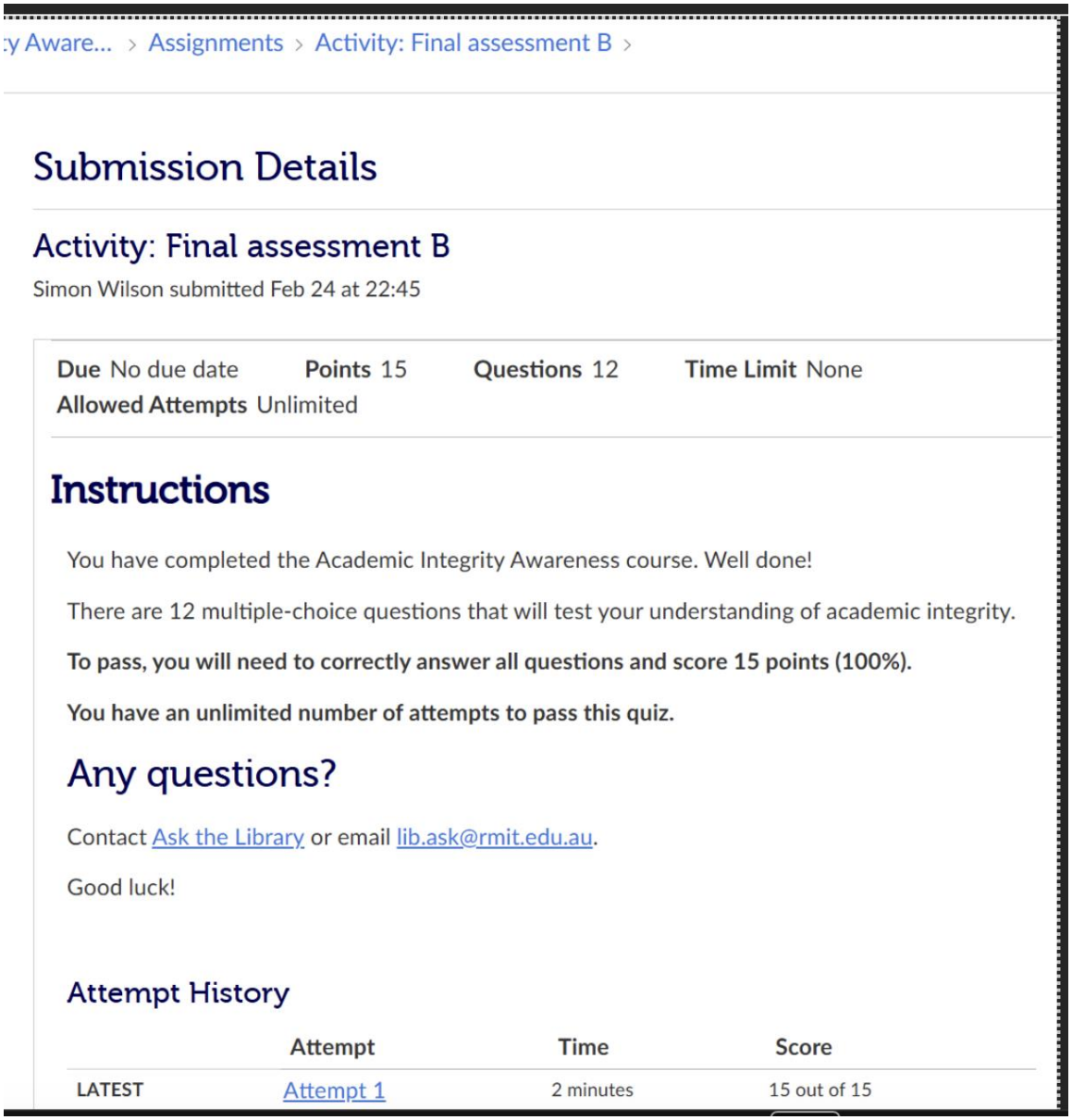
In conclusion, this assignment has far exceeded the expectations of a standard university project. It has shaped how we view cybersecurity as a human-centred, governance-driven field, and equipped us with skills directly applicable to real-world consulting, risk management, and policy development roles. We are confident that the insights, communication abilities, and strategic thinking we developed through this experience will serve us far beyond this course—and well into our professional futures.

Appendix G: Academic Integrity

Phranavh Alathur Sivaraman



Simon Wilson


y Aware... > Assignments > Activity: Final assessment B >
Submission Details
Activity: Final assessment B
Simon Wilson submitted Feb 24 at 22:45
Due No due date
Points 15
Questions 12
Time Limit None
Allowed Attempts Unlimited
Instructions
You have completed the Academic Integrity Awareness course. Well done!
There are 12 multiple-choice questions that will test your understanding of academic integrity.
To pass, you will need to correctly answer all questions and score 15 points (100%).
You have an unlimited number of attempts to pass this quiz.
Any questions?
Contact Ask the Library or email lib.ask@rmit.edu.au.
Good luck!
Attempt History
Attempt
Time
Score
LATEST
Attempt 1
2 minutes
15 out of 15