

Building Cyber Resilience Through Application Control



The Association of
Independent Schools
of New South Wales





Marcus Claxton

Manager: Cyber Security and
Infrastructure Advisory Services

“We don’t support
technology, we support
people in the use of
technology!”



School: A Discrete Complex System





* * * * *

Is Shadow IT A Problem?

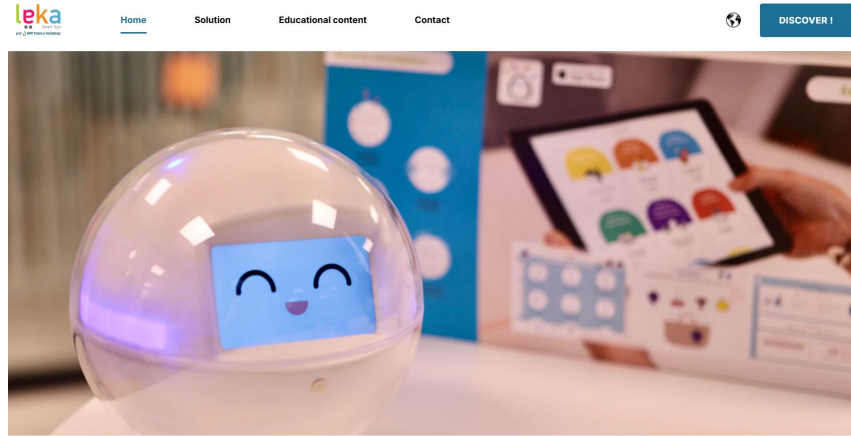
Welcome Aboard – Now Make This Work

The Case Of The Leka Robot

My first month in the role

An unexpected brown box

Enthusiastic Teaching Staff



OUR MISSION AT LEKA

HELPING EXCEPTIONAL PEOPLE LIVE EXCEPTIONAL LIVES!

Welcome Aboard – Now Make This Work

Question Time:

Why this?

Were IT consulted?

Documentation?

What did it cost?

Did you follow the process for adoption of new tech?



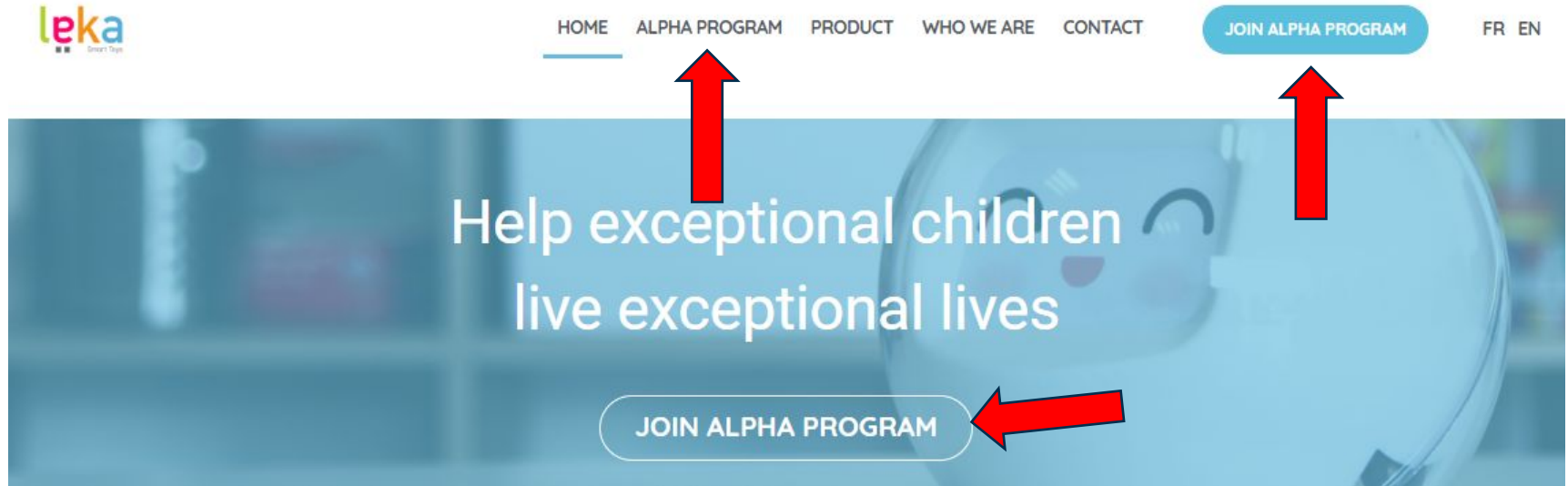
A ROBOTIC COMPANION

The robot allows...

- ✓ To promote engagement in learning
- ✓ To offer sensory stimulations tailored to individual needs
- ✓ To act as a mediator between the accompanied individuals and professionals

[Learn more](#)

The leka website – August 2018



You do know that an alpha version of a product won't do what you are expecting it to do....don't you?



Why Am I Telling You This Story?

The Human Perspective



School Shadow IT

- **Unauthorised Technology Use**
 - A new fancy IoT device in TAS or Science
 - Signing up to a new online tool to analyse student performance
 - A new AI image generation tool in Visual Arts
 - Accessing school systems through a personal computer at home....
 - Signing up to, and using Deepseek
- **Bypassing Established Processes**
 - Accessing systems bypassing controls

Whenever A New Technology Is Adopted:

Processes/Procedures

- Year End Rollover
- Access Management
- Acceptable Use

Risk

- Data Security, Privacy And Compliance
- Increased Complexity
- Data Sovereignty
- Lack Of Compliance With Security Policies
- Potential For Malware Infiltration



Financial Cost

- Operational Budget
- Consumption Costs
- Development Costs
- Additional Features



Support Overhead


- Business As Usual End User Support
- Onboarding And Configuration
- Updating And Patching



Training Requirements

- New Staff/Student Training
- New Feature Training



A close-up photograph of a person's hands using a screwdriver to turn a door handle. The person is wearing a dark long-sleeved shirt. The background is a bright, out-of-focus white. The text "Every Additional Application Is Another Potential Open Door..." is overlaid on the left side of the image.

Every Additional Application Is
Another Potential Open Door...

The Dichotomy Of Shadow IT



Mastering The Shadow

1

Leadership

2

Policy And
Process

3

Staff
Engagement

4

Review
Process

5

Tools

Leadership

Everything Rises And Falls On Leadership:

- Risk conversations
- Executive team
- Whole of school strategic perspective
- Cyber Secure Culture
- ICT leader to review all ICT purchases

Cyber Security – An Organisational Risk, Not
Just An ICT Problem

Policy And Process

Formalisation:

- Clearly articulated in IT Policy
- Alignment with Strategy
- Simple business case
- Well defined and simple request process
- Maintain an Application Catalogue
- ICT owns all ICT licensing in the budget

Name	Grouping	Lifecycle Status (Testing/Production/Deprecated /Decommissioned)	Usage	Platform
1password	SaaS	Production	Password management	SaaS
Abnormal Security				
Access MicrOpay				
ADFS				
Adobe Creative Cloud				
Adobe Digital Edition				
Adobe eSign				
School Website	Website	Production	www.websiteURL.edu.au	Wordpress

Name	Organisation Responsibility	Technical Responsibility	SME	Access IP / URL
1password	Business Manager	ICT Manager	Sys Admin	
Abnormal Security				
Access MicrOpay				
ADFS				
Adobe Creative Cloud				https://account.adobe.com/
Adobe Digital Edition				https://adobe.com
Adobe eSign				
School Website				https://www.websiteURL.edu.au/

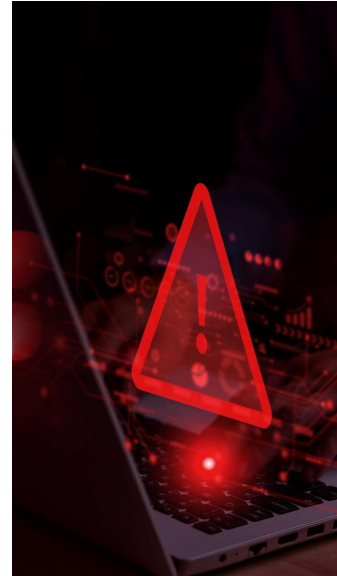
Upfront effort and regular reviews

Stakeholder Engagement

Don't become the department of NO:

- Walk the journey with staff
- Engage with the why
- Part of Cyber Security Awareness Training
- Guidance in favour over enforcement

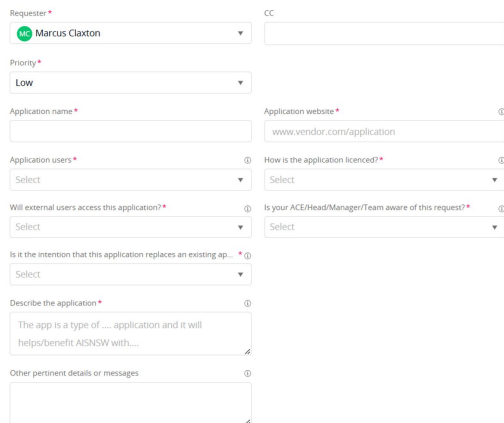
C'mon, let's work as a team and do it my way.....



Tech Review Process

Our goal is Professional Learning that is:

- Read the T&Cs and Privacy Policies
- Safer Tech 4 Schools (ST4S)
- Threat Intelligence
- Consult peer networks such as MITIE
- Consult legal advice
- Refer to organisational, ICT or security strategy



A screenshot of a web form titled 'Tech Review Process'. The form is divided into two columns. The left column contains fields for 'Requester *' (with a dropdown menu showing 'Marcus Claxton'), 'Priority *' (with a dropdown menu showing 'Low'), 'Application name *', 'Application users *' (with a dropdown menu showing 'Select'), 'Will external users access this application? *' (with a dropdown menu showing 'Select'), 'Is it the intention that this application replaces an existing ap... *' (with a dropdown menu showing 'Select'), 'Describe the application *' (with a text area containing 'The app is a type of ... application and it will help/benefit AISNSW with...'), and 'Other pertinent details or messages'. The right column contains a 'CC' field, an 'Application website *' field (with a text area containing 'www.vendor.com/application'), 'How is the application licenced? *' (with a dropdown menu showing 'Select'), and 'Is your ACE/Head/Manager/Team aware of this request? *' (with a dropdown menu showing 'Select'). Each field has a small icon to its right.

Are we confident that the new tech is safe and secure enough?

Tools

Control:

- Microsoft Intune/Jamf – Mobile Device Management (MDM)/Mobile App Management (MAM)
- Microsoft Cloud App Discovery
- Airlock Digital, Threatlocker, etc
- Staff local administrator access?

Time and resource cost to implement and utilise.....

Mastering The Shadow

1

Leadership

2

Policy And
Process

3

Staff
Engagement

4

Review
Process

5

Tools



Back to The Cuckoo's Egg: What if?

Essential Eight Controls	ISO 27001:2022 Controls
Application Control – Prevents unauthorised software execution.	A.5.13 – Network Security – Protects internal and external network access.
Patch Management – Mitigates vulnerabilities that attackers exploit.	A.5.16 – Identity Management – Ensures secure user authentication and authorisation.
Privileged Access Management (PAM) – Restricts administrative privileges.	A.5.23 – Information Security for Cloud Services – Secures data in cloud environments (if applicable).
Multi-Factor Authentication (MFA) – Enhances account security beyond passwords.	A.8.8 – Logging and Monitoring – Supports real-time detection of unauthorised activities.
Continuous Monitoring and Logging – Identifies anomalies in real time.	A.5.7 – Threat Intelligence – Leverages threat intelligence to anticipate and respond to threats.
Regular Backups – Ensures data recovery and minimises impact from breaches.	A.5.30 – ICT Readiness for Business Continuity – Ensures ICT resilience during incidents.