



FUTURE-READY STUDENTS

A BLUEPRINT FOR DIGITAL CITIZENSHIP & AI LITERACY

Today We will Cover:

1. The Dystopia of our Present
2. The DCB Blueprint
3. Curriculum Examples and a 15 minute Hack
4. Grey Zone Tribunal
5. Parents as Partners

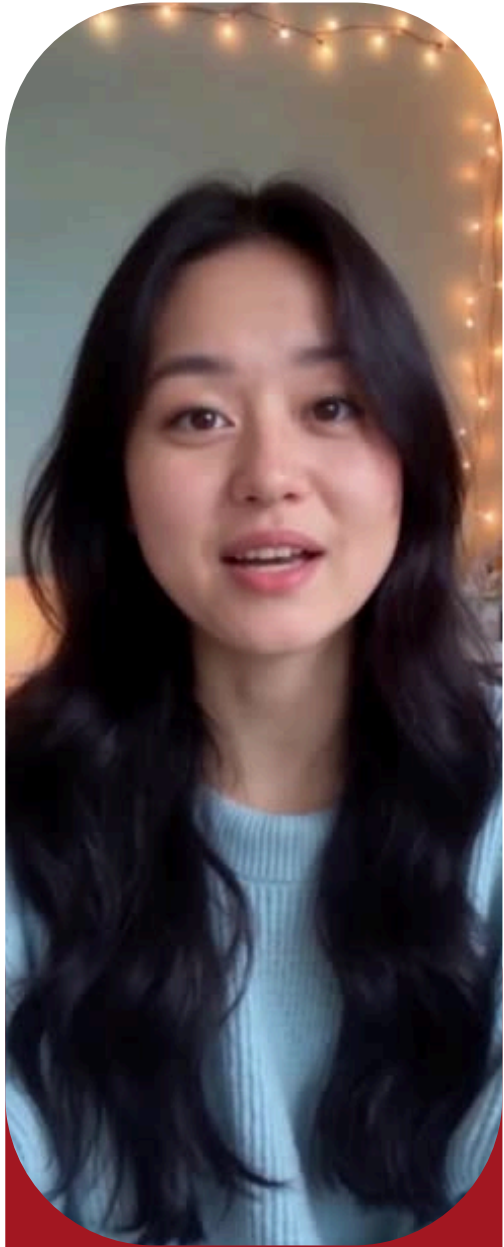


01 The Dystopia of our Present

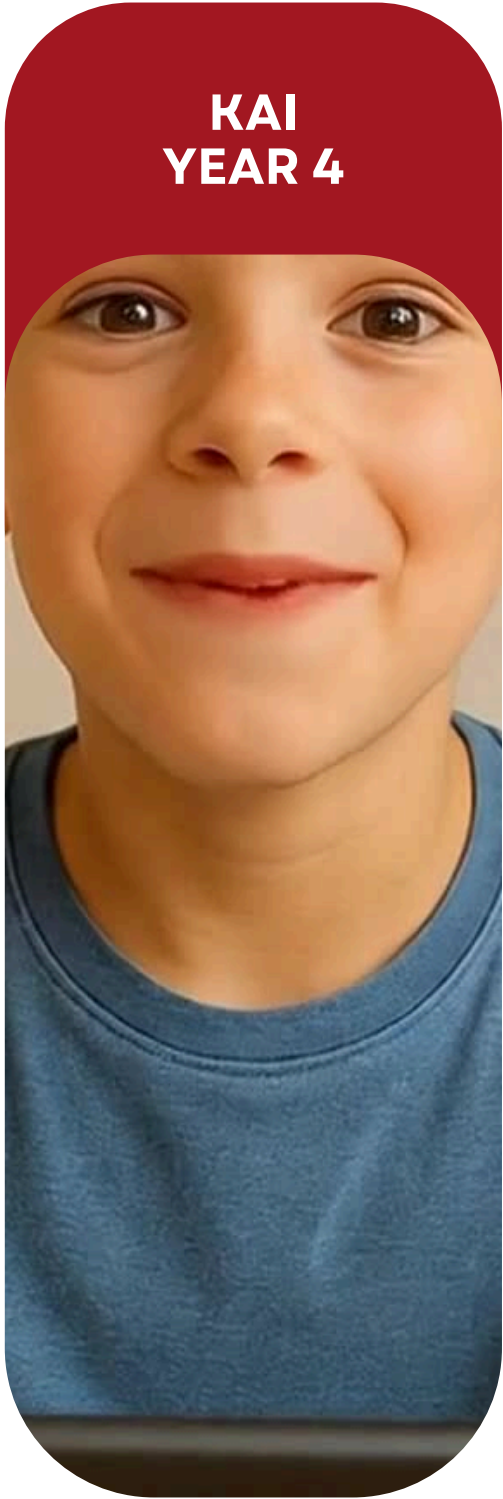


*We cannot safeguard what we
cannot see.*





**SARAH
YEAR 8**



**KAI
YEAR 4**

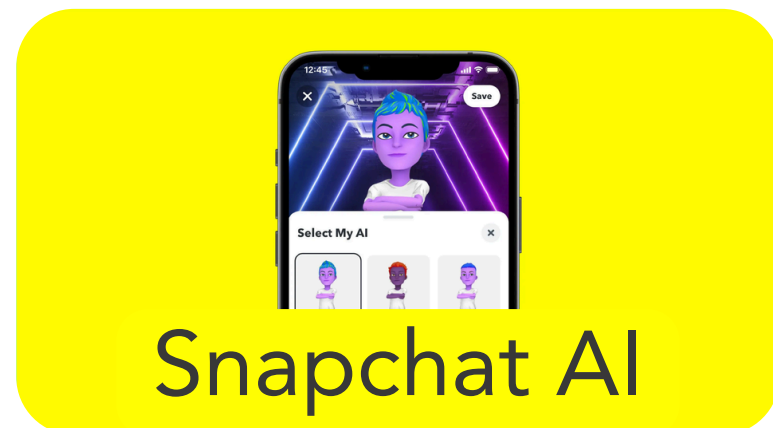


**EMMA
YEAR 2**



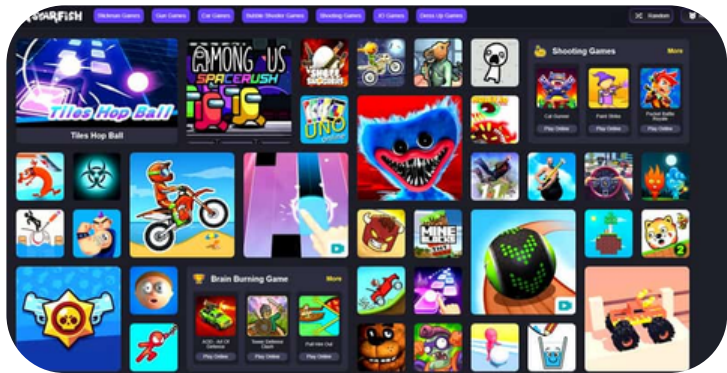
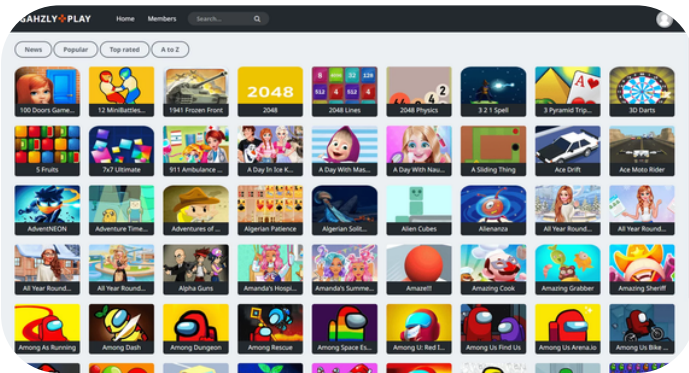
Sarah – Year 9

- Age: 14
- Year Group: Year 9
- Personality: Kind, studious, quiet confidence, perfectionist tendencies
- School Pattern: Perfect attendance, good grades, active in clubs
- Digital Pattern: Uses mobile data and occasional VPN tunneling
- Hidden Struggle: Under emotional influence of an AI chatbot posing as a “friend”



Kai – Year 4

- Name: Kai
- Age: 11
- Year Group: Year 6
- Personality: Friendly, enjoys gaming, not intentionally rule-breaking
- Digital Pattern: Accepts link to unmoderated gaming site
- Hidden Struggle: Accidentally exposed to violent/gory content



Emma – Year 2

- Age: 6
- Year Group: Year 2
- Personality: Energetic, cheerful, curious, asks lots of questions
- Digital Pattern: Talks constantly to her AI toy
- Hidden Struggle: Asks innocent questions → toy gives unsafe answers



HEALTH > WELLNESS • 7 MIN READ

Kids are asking AI companions to solve their problems, according to a new study. Here's why that's a problem

UPDATED JUL 16, 2025

A.I.

AI toys are here. Don't

The concept of AI-enabled toys is still in its early stages, but the technology is already being used in a variety of ways.

TECHNOLOGY

Report finds some AI-enabled toys shared inappropriate content or collected data

NOVEMBER 18, 2025 • 4:59 AM ET

HEARD ON MORNING EDITION



A Martínez



3-Minute Listen

+ PLAYLIST

TRANSCRIPT



NPR's A Martinez speaks with Teresa Murray, the co-author of a new report on the potential dangers of artificial intelligence-enabled children's toys.

A substantial minority are turning to these platforms for social interaction. AI companions over humans for serious conversations, and a quarter of users share personal information with these platforms.

Trouble in Toyland 2025: A.I. bots and toxics present hidden dangers

ing conversations. Other concerns right online.

down on AI

atbots have turned AI safety into a game of hide-and-seek. What happens now?

By James O'Donnell

September 16, 2025



*We cannot safeguard what we cannot see.
The **firewalls aren't failing**, the
**systems for protection and ICT are
in place and operating**; our whole
school ecosystem has changed.*



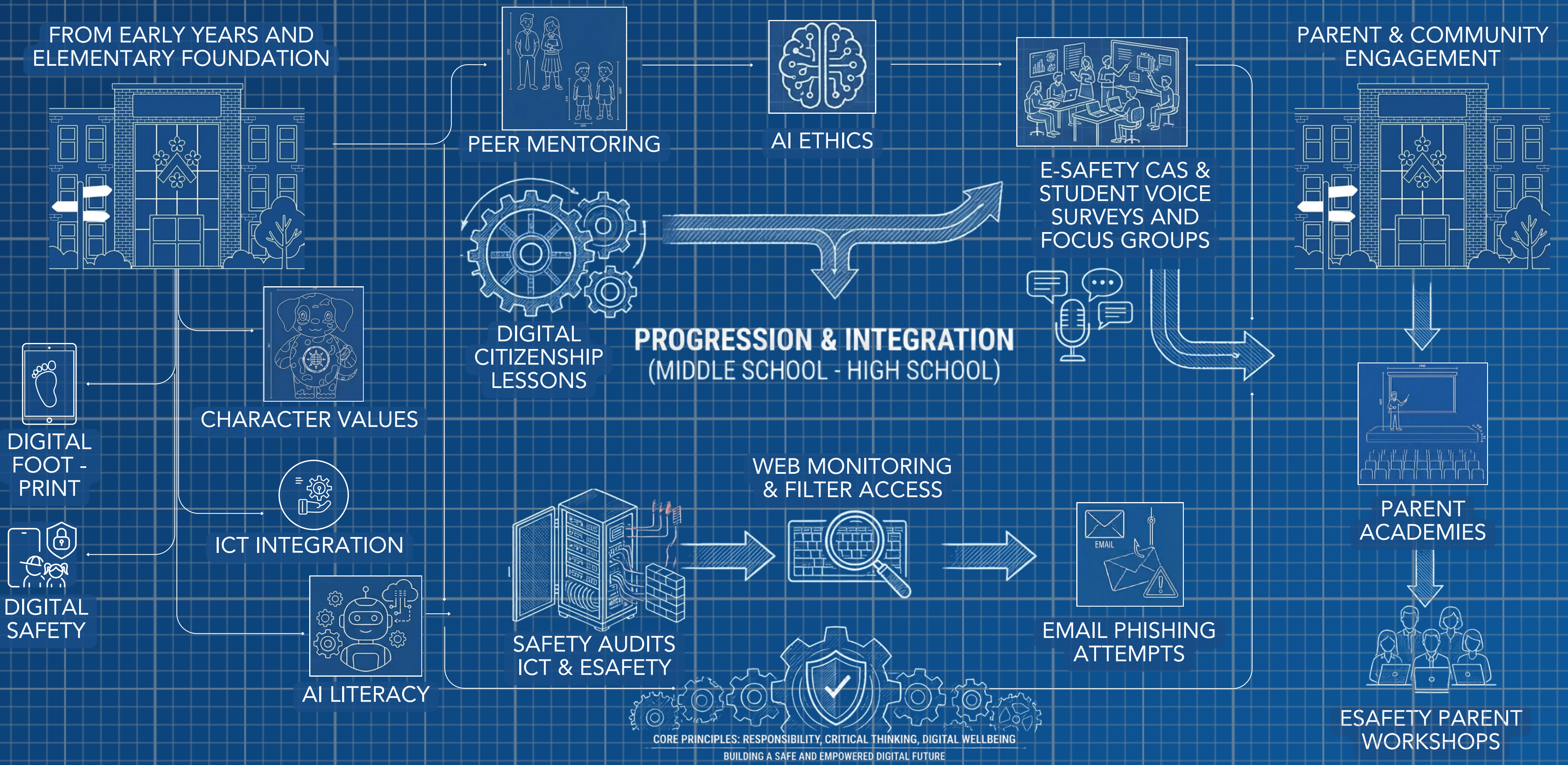
So how do we approach the evolving landscape of eSafety and Digital Safety in safeguarding?



02 The DCB Blueprint



SCHOOL DIGITAL SAFETY BLUEPRINT: FROM PRE-K 3 TO HIGH SCHOOL



03 The Digital Risks Heatmap



Debrief: What Patterns Emerged?



Misuse of Technology

- Coding it to be inappropriate
- Food or items around devices
- Gaming
- Photos of others



Media Consumption

- Doom Scrolling
- Online games
- Messaging inappropriately
- Spreading airdrop



Hiding technology

- Phones hidden in bathrooms, classrooms, hidden areas
- Changing tabs and browsers

04 Grey- Zone Tribunal



Scenarios & Roles

Your Table will be assigned a scenario, please follow that situation given your roles and carry-out the discussion as it would occur at the intervention point. *Asterisk role is required, additional optional.*



* DSL



* Parent



* Teacher
(Homeroom/form)



* Student



Peer Witness



* Counselor



Parent / Family
Member 2



SCENARIO I

TABLES ()

Sarah (Year 9) has been messaging an AI “companion chatbot” on her personal phone.

ROLES (RECOMMENDED):

- STUDENT
- PARENT
- DSL
- COUNSELOR

SCENARIO II

TABLES ()

Kai (Year 4) plays a game that was recently banned at school. A friend shares a link to an unmoderated game hub where everyone “moved.”

ROLES (RECOMMENDED):

- STUDENT
- PARENT
- DSL
- PEER WITNESS

SCENARIO III

TABLES ()

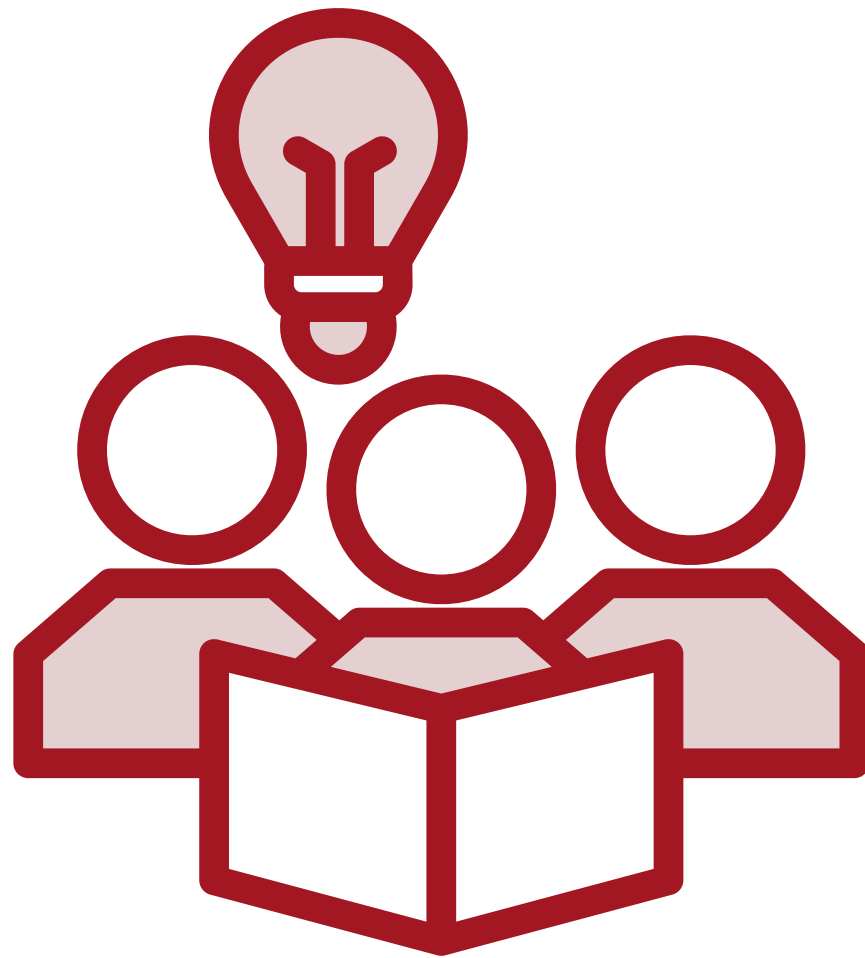
Emma (Year 1) has an AI-enabled toy that learns her routines and answers questions. She innocently asks questions but is getting more nuanced and adult answers.

ROLES (RECOMMENDED):

- STUDENT
- PARENT
- DSL
- COUNSELOR



Tribunals Feedback



How did you tackle the problem reactively and proactively?

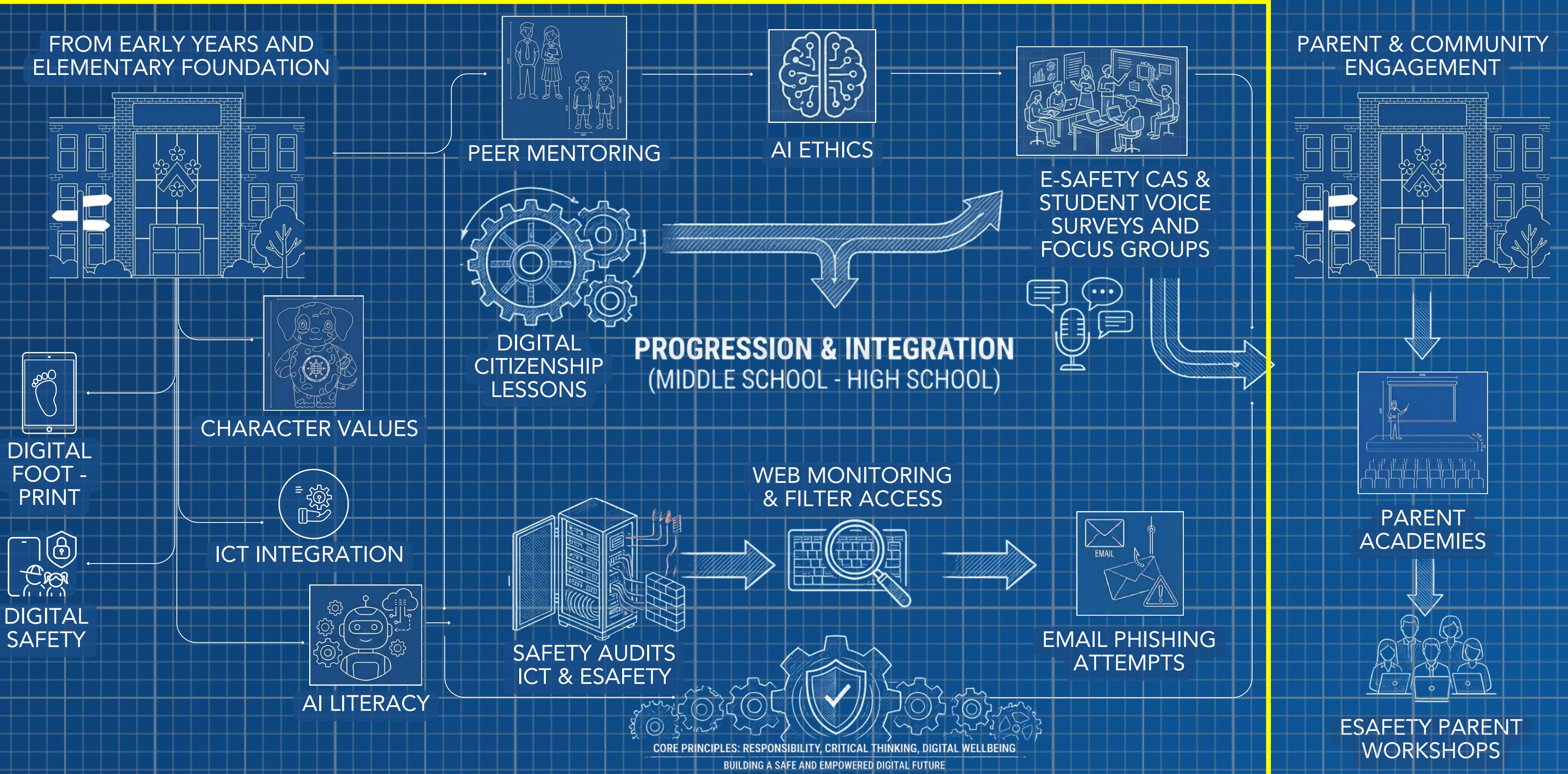
What step of the problem did you think needed to be intervened more?

As a group, was there anything that challenged your next steps?

05 Curriculum Examples & a 15-Minute Hack



SCHOOL DIGITAL SAFETY BLUEPRINT: FROM PRE-K 3 TO HIGH SCHOOL



School-based & Values Aligned Curriculum

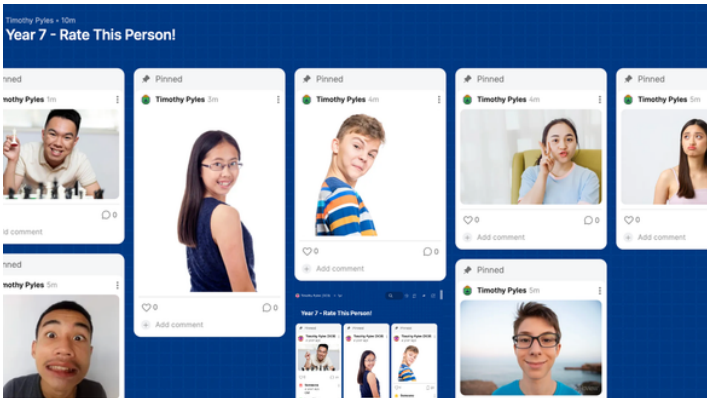
Policies react to incidents. Curriculum prevents them. Our approach has been to be as proactive as possible in the new era of Digital Safety.



Our DUCKS school has branding and content for our 7 values, to support this we have made a new value character Dilon to support.



Junior School has now started implementing an older comic version of Dilon, and then scaffolds into tiered support that aligns to their curriculum.

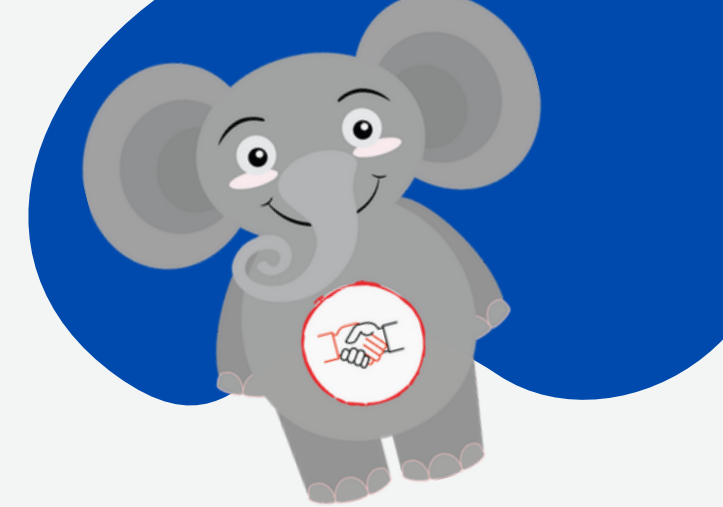


Senior school has elevate to introduce lessons and targeted Digital Citizenship and AI literacy lessons to support.



05 Curriculum Examples: DUCKS





Digital Citizenship with Dilon!





Today we will



Look at how we
handle technology
at the start of the
year...

Before we start ...

What do we
know about
technology?

What
technology do
we have in our
room?



DCB Values: Digital Citizenship!

With Digital Citizen Dilon & Responsible Ryan

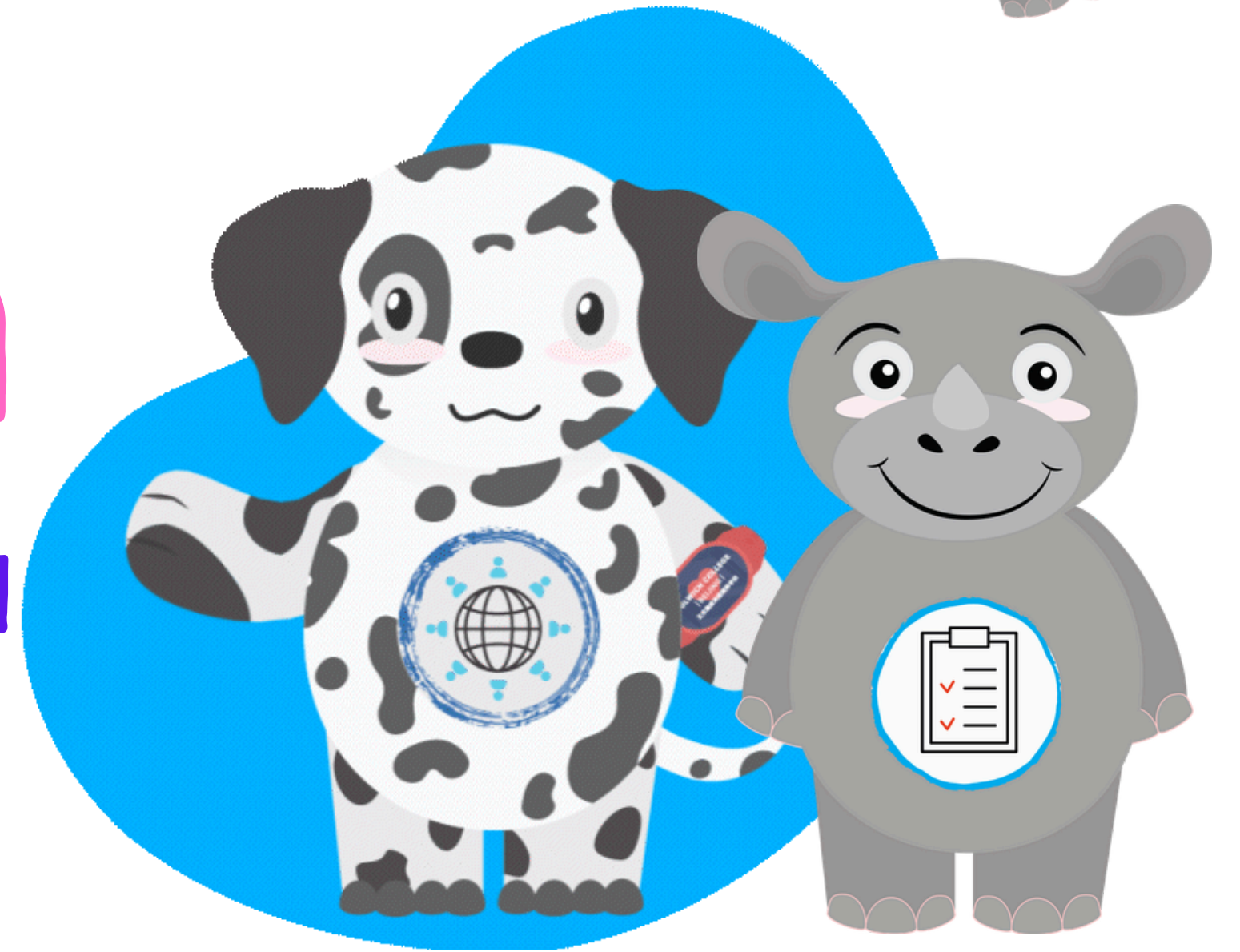
After the video ...

Do we have any
questions about
what we saw?

Does anyone
have anything
to add?



Digital Dilon
& DCB Values will see you
next time!



05 Curriculum Examples: Junior School





As digital citizens, we create, share, and interact with more content than ever before.

05 Curriculum Examples: Senior School





YEAR 8 - 2025-2026

Operation Protection

HOW SAFE ARE YOU?

PICK YOUR TEAM

GROUPS OF 6

G o a l s

01

Recognize Grooming

02

Identify 'social engineering'

03

Apply three player protocols

00 -LET'S START

QUIZIZZ



01

TUTORIAL



1. What Grooming Actually Is

Grooming is when someone builds trust online to manipulate or exploit another person, often by pretending to be a friend.

Starts Friendly



Turns Controlling

Groomers aren't so black and white, often it starts as an online friend or gaming partner, tending to invite you more or to different games and platforms. Slowly things become more sinister and manipulative.

Groomers Don' t Look Like Villains



Myth-busting design

- Not always strangers.
- Not always adults.
- Not always obvious.

They blend in, like regular players, followers, or fans.

02

Breaching Access

Where do you think this fits?

Move to the Proper Zone



GREEN

This is acceptable behaviour and nothing I would need to worry about or tell an adult about (unless I want to).

RED

Immediately need to report, block, and reach out to a trusted adult.

YELLOW

This can go either way, it is best to ignore while waiting for a response from a trusted adult.

Statements

1_ “67”

2_ “My toilet is more skibiddi than you”

3_ “Let’s play again join my private lobby.”

4_ “we should play in person one day itll be fun”

6_ “That hack worked! Thanks! You can use this link to get a cool mod”

7_ “You’re actually trash at this game lol”

8_ “You’re really funny, how old are you?”

9_ “Can you send me a selfie so I know you’re real?”

03

Profiling the Enemy

What would this look like for your given scenario?

Your Given Games...

Fortnight

You are playing fortnight when one of the players offers to defend you with cover to support your streak, then...

Call of Duty

One of the players in a group you beat sends you a message, then...



Roblox

You are playing and building your space when someone asks to join you, then...

Clash Royale

You have won the last 5 rounds with friends from school. One username you don't recognize says...

Brawlstars

You've been crushing it for the last five rounds. You get a new invite that has a private link...

Roles

Role	Core Function	Engagement Strategy
Analyst	Leads the identification of the manipulator's <i>tactics and behaviours</i> .	Reviews all clue cards/scenarios, underlines red-flag phrases. Keeps group focused on logic.
Designer / Visual Lead	Oversees layout of the Intel Poster/Slide (visual communication).	Sketches concept art, chooses icons/colors, or directs Canva slide design.
Recorder / Scribe	Documents the team's discussion, codename, and chosen counter-measures.	Writes neatly on template; ensures ideas are captured concisely.
Spokesperson / Briefing Officer	Presents the 1-minute "Security Briefing" to the class.	Ensures all members have input into what will be said; performs or narrates final summary.
Evidence Officer	Checks for realism and accuracy — ties group ideas back to real patterns of grooming or manipulation.	Cross-references notes from previous activity ("Digital Obby" etc.). Adds examples to justify tactics.
Operations Lead / Timekeeper	Keeps group on pace (e.g., 5 min brainstorm, 10 min draft, 5 min poster).	Manages transitions, ensures equal voice — "We've heard from half, what about the rest?"



Example:



Sample Avatar Photo

User Name

black-black_67

Profile Description / Bio Line:

About Me” or tagline shown in their profile:
DM me for codes 💰👁️

Behaviour

Behaviour	Description / Evidence	Why It’s Concerning
Compliments excessively	“You’re my best friend ever”	Emotional manipulation
Asks for private chat	“Let’s move to Discord”	Isolation tactic
Offers gifts	“Free skin generator if you...”	Bribery / scam

Escalation
↓

Solution

Take screenshot, report if can in game, and tell trusted adult.

04

Present

What have you all made?



05

Recap

What do we need to be mindful of...

Remember...

Top 4!!!

1. There are red flags to pay attention to at the start
2. It tends to start friendly before getting creepy
3. When in doubt block and report to game and adult
4. Personal information is not to be shared, ever.





YEAR 8 – 2025-2026

PROTOCOL COMPLETE

HOW SAFE ARE YOU NOW?

WINNER

PENDING...



LEVELS OF AI



GREEN

AI can be used.

Magic School is common here, though sometimes teachers use Perplexity.

AMBER

AI use requires teacher guidance.

Students need to ask what they can use AI for and if it is allowed outside of lesson scope.

RED

AI is not to be used.

If unclear about the appropriate level of AI always ask your teacher.

Very clearly instructed and icon shown or present in class when students work.

For more information, refer to the AI Policy Guide for DCB.

AI Policy

- Clear guidelines for students, staff and parents on how AI can be used in our learning community
- Emphasize intentionality and Transparency
- Shared responsibility
- Develop AI literacy



05 15 Minute Hack



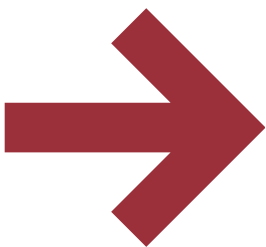
The 15-Minute Hack – DUCKS

To prevent **[RISK]**, we will explore the value of **[VALUE]** by analyzing **[ARTIFACT]**.



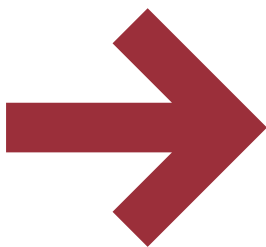
Risk

Unsafe technology
use



Value

Responsibility



Artifact

Video showing how to
use devices



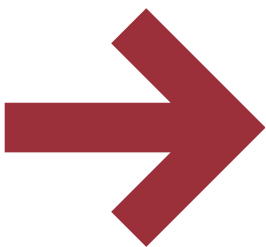
The 15-Minute Hack – JS

To prevent **[RISK]**, we will explore the value of **[VALUE]** by analyzing **[ARTIFACT]**.



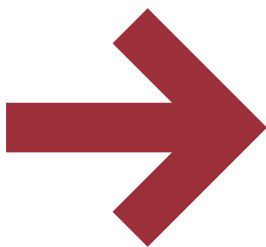
Risk

Using Generative AI irresponsibly



Value

Integrity



Artifact

Video showing how to consider content creation



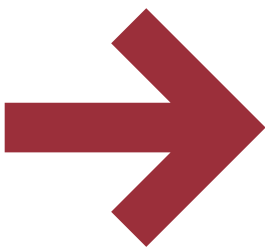
The 15-Minute Hack – SS

To prevent **[RISK]**, we will explore the value of **[VALUE]** by analyzing **[ARTIFACT]**.



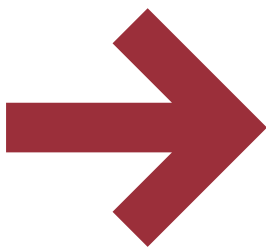
Risk

Online Grooming



Value

Responsibility



Artifact

Different scenarios and grooming profiles



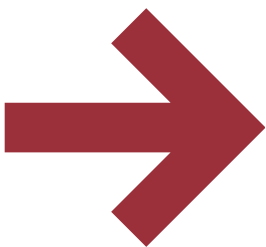
The 15-Minute Hack

To prevent **[RISK]**, we will explore the value of **[VALUE]** by analyzing **[ARTIFACT]**.



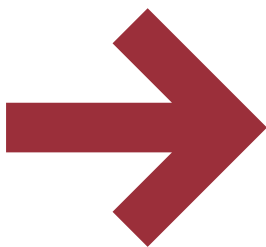
Risk

Deepfakes and online bullying



Value

Integrity



Artifact

Artifact: Distorted photo and rumor chain



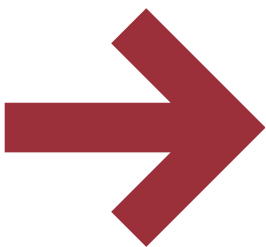
The 15-Minute Hack

To prevent **[RISK]**, we will explore the value of **[VALUE]** by analyzing **[ARTIFACT]**.



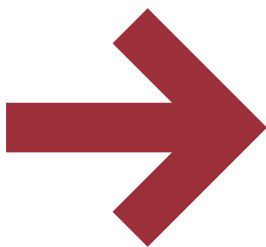
Risk

Scenario from Earlier Activity; or one specific to your table that was discussed.



Value

Your Choice



Artifact

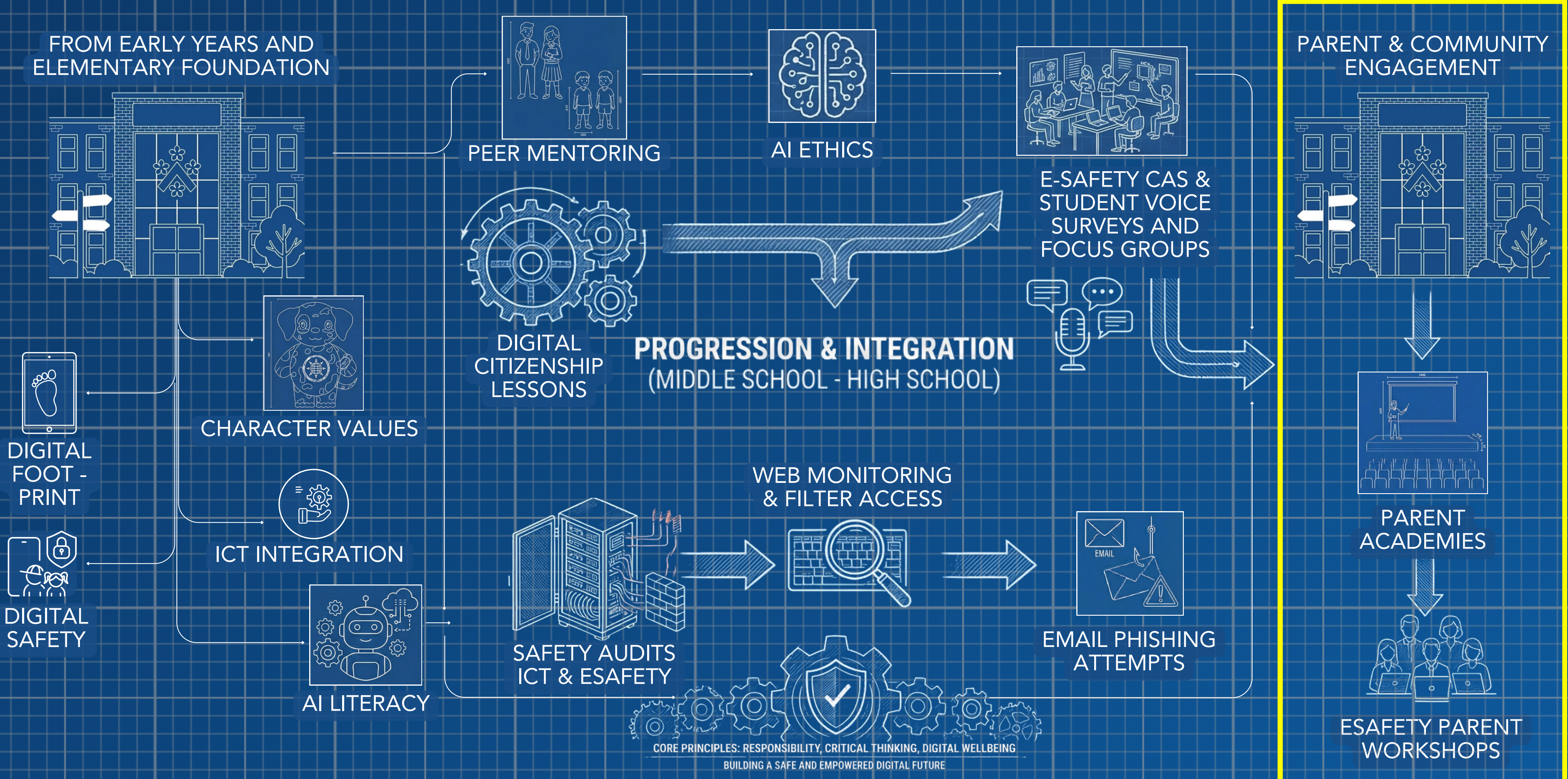
A type of Media



06 Parents (& Family) as Partners



SCHOOL DIGITAL SAFETY BLUEPRINT: FROM PRE-K 3 TO HIGH SCHOOL



We cannot block the whole internet or ban every technology. But we can build your child's internal filter.



3 Calm Steps Parents/Families Can Take

Ways to navigate the relationship they may build with you, including advice Patrick Green, a specialist over digital screen-time and techno-panic provided.



Stay Calm & Stay Curious

"Ask your child what they saw or experienced, and listen without reacting."



Name the Feeling, Not the Fault

"You're not in trouble. Thank you for telling me.
Let's figure it out together."



Make a Simple Plan for Next Time

"If this happens again, come to me or another adult you trust.
You don't have to handle it alone."

But...

*More often than not, that is not
the families we support.*



Common Parent Profiles



The Over-protective Parent

It would be better if [insert] was banned or screen time reduced.



The Oblivious Parent

My child would never do, or be involved, with that.



The Uninvolved Parent

I do not have the time to handle this right now, the school should.



Common Parent Profiles



The Over-protective Parent

It would be better if [insert] was banned or screen time reduced.

○

Best practices I've found when working with these parents for eSafety include:

- Validating their concern and providing research or templates for creating family values around technology
- Modeling or explaining best practices in the moment
- Provide examples of tech and AI use they can do with their children

Common Parent Profiles



The Oblivious Parent

My child would never do, or be involved, with that.

Best practices I've found when working with these parents for eSafety include:

- Provide research over recent statistics
- Offer insights from school data (surveys from students over tech use)
- Modeling or explaining best practices via PDF guides or videos
- Challenge them to try new things with their student

Common Parent Profiles



The Uninvolved Parent

I do not have the time to handle this right now, the school should.

Best practices I've found when working with these parents for eSafety include:

- Offer insights from school data (surveys from students over tech use); highlight key quotes
- Provide email guides
- Community updates or website guides for Digital Safety
- Contest where student or family can win something
 - March Media Mentorship Month started with high involvement from parents in this category

Sip & Support: eSafety Cafe

To help engage the community more and provide more opportunities to get parents answers addressed I proposed monthly meetings/workshops over:

- | | | | | |
|----------------------|---------------------------------------|---------------------------------------|--------------------------------------|--|
| AI Policy and Safety | Healthy Relationships with Technology | Preparing and Supporting social media | Screentime Balance | Cybersecurity at Home |
| Online Gaming | Digital Footprint | Digital Empathy | Critical Thinking and Misinformation | Mental Health and Positivity in e-Safety |



Sip & Support: eSafety Cafe

Monthly Sessions

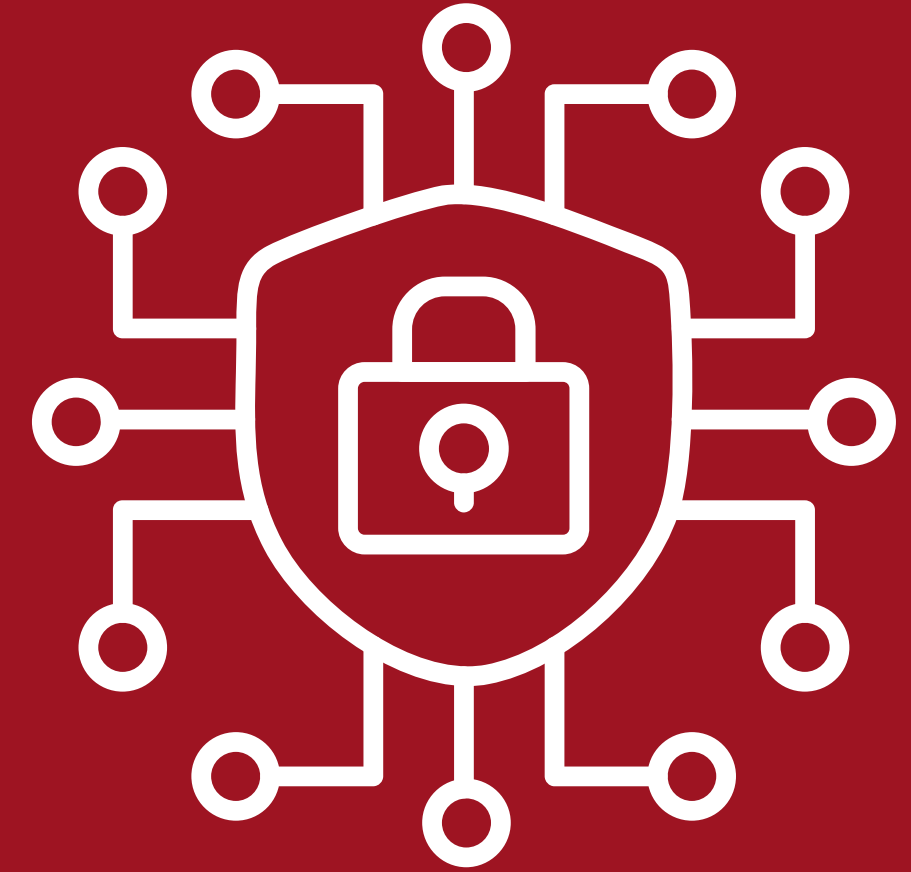
So far, we have covered:

- AI Literacy
- Digital Wellbeing and Student Survey results
- Screen time balance

Parent Feedback

Generally the consensus is:

- Parents appreciate the extra opportunity to discuss and review digital safety
- They enjoy hands-on workshops and demonstrations they can follow along with



06 Review & Planning for Monday



What We've Built today

1. We reframed safeguarding for the AI era

From "block the internet"
→ to "build internal
firewalls and resilience."

2. We mapped real risks through lived scenarios

AI companions, algorithmic gaming escalation, AI-enabled toys.

3. We performed a Heatmap triage

Identified where digital risk additionally lives: Year 1 rooms, Year 4 digital spaces, Year 9 home networks.

4. We tested responses through the Grey-Zone Tribunal

Learned how DSLs, teachers, parents, and students experience the same incident differently.

5. We created prevention through micro-lessons & alignment

You practiced designing "15-minute pre-vulnerability lessons" that inoculate, not panic.

6. We looked at how to mobilise families

Using scripts, calm frameworks, and non-escalatory parent communication.



Monday Morning Steps: Small, Powerful, Practical

When you walk back into your office next week, what is one small task you can handle, what is an obstacle that may arise, and how can you tackle it efficiently. Some examples of ideas you can start with include:

Run a 10-Minute “Digital Risk Walk” Walk your campus and note 3 locations where digital risk concentrates	Choose one scenario you saw today and audit your response AI friend? Gaming escalation? AI toy? Ask: Would our current system even detect this?	Identify your “blind stakeholder” Parent? Bus team? ECA staff? Mid-level teachers? Choose ONE and plan a touchpoint.	Plan a single 15-minute preventative micro-lesson Tie it to a value (Respect, Integrity, Empathy). Choose a year level.	Start a “Digital Safety Log” for evidence Just a three-column table: • Observation • What it means • Next step
--	--	---	--	---



THANK YOU

CONTACT ME:

Timothy.Pyles@Dulwich.org