Cybernetic Shield

Beyond Cyberbullying

The Online Safeguarding Risks Schools Are Now Managing

UQ Webinar

Jessica Sears

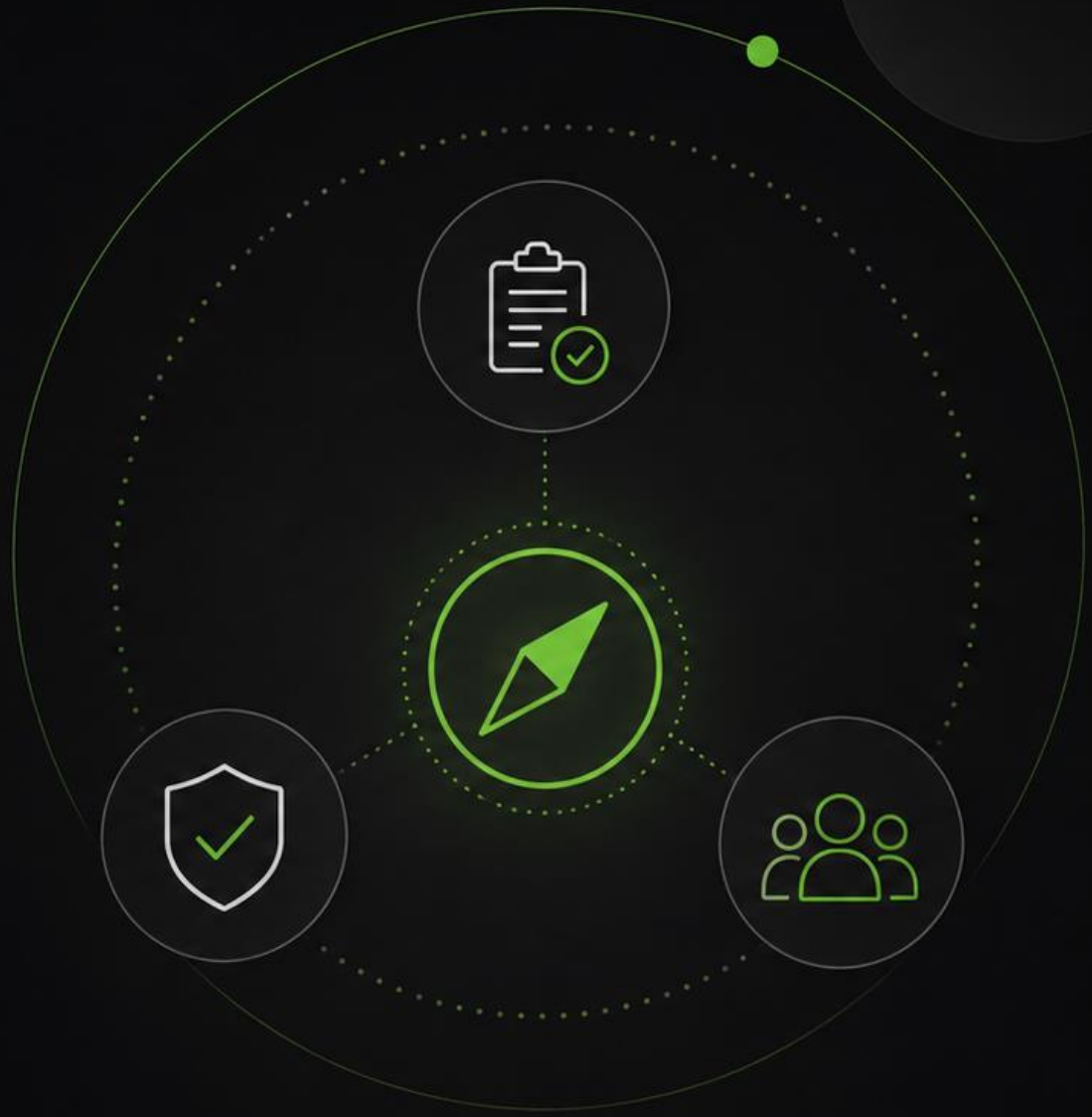
Cybernetic Shield

Cybernetic Shield

What this session is really about

This is not a session about becoming an expert in every platform.

- Recognise when an online issue may be becoming a safeguarding concern
- Take safe and proportionate initial action
- Know when the school needs additional support



Cybernetic Shield

Who Cybernetic Shield is

Prevent

- Student education
- Staff and parent resources
- Preparedness and response planning

Respond

- 24/7 incident support
- Safeguarding triage
- Practical response guidance

Recover

- Investigations
- Evidence and content support
- Psychological and recovery services

Support across the full incident lifecycle

Cybernetic Shield

Four families of online safeguarding risk

Created or manipulated content

- AI-generated images
- Deepfakes
- Impersonation
- Fake accounts

Coercion, exploitation and sexual harm

- Grooming
- Sextortion
- Image-based abuse
- Coercive communication

Cyber-enabled targeting and compromise

- Account takeover
- Doxing
- Scams
- Identity misuse

Social, behavioural and wellbeing harms

- Harmful communities
- Hate and extremism
- Misogynistic content
- Digital wellbeing concerns

These categories help organise risk, but incidents often cross more than one domain.

Cybernetic Shield

Incidents rarely remain in one category

A single incident can move through multiple domains.

Fake account created	Humiliating content shared	Peer harassment	Threats received	Student avoids school	Parents contact leadership	Reputational and safeguarding concern
Impersonation	Image-based abuse	Cyberbullying	Sextortion or coercion	Wellbeing impact	Safeguarding concern	

One incident. Many impacts.

It may be a behaviour issue, safeguarding concern, wellbeing matter, cybersecurity issue and more.

What is actually happening online?

Cybernetic Shield

Australian children and adolescents are already facing a broad mix of online harms.

52%

experienced cyberbullying

children aged 10–15

14%

experienced online grooming-type behaviour

children aged 10–15

8%

experienced image-based abuse

children aged 10–15

7%

had a fake online identity or profile made of them

without their permission

11.3%

experienced sexual extortion

adolescents aged 16–18

$2.18b

reported scam losses in Australia in 2025

broader threat context

Schools are not just managing cyberbullying. They are increasingly managing overlapping safeguarding, wellbeing and cyber risks.

Sources: eSafety Commissioner research, 2026; National Anti-Scam Centre / Scamwatch, 2025 report.

Why schools are being asked to manage it

It may not begin at school, but it can quickly become a school issue.

Students involved attend the same school

Distress affects attendance or learning

Content spreads through school peer networks

School images, uniforms or staff are used

Conflict moves into classrooms or the playground

Parents expect the school to intervene

The school holds information relevant to safety

Online behaviour impacts learning, wellbeing and school culture

Parents contact leadership and expect a response

The school may hold information relevant to student safety

The impact is what matters.

Focus on the child's safety, wellbeing and ability to participate in school.

Early-stage harm rarely arrives clearly labelled

What schools may initially hear.

"It was only a joke."	"It is friendship drama."	"They sent it willingly."	"It happened outside school."	"It is just a group chat."	"They have sorted it out."
					
Is someone being pressured?	Is there a pattern?	Is material being shared?	Is the student frightened?	Is someone losing control of the situation?	Is the behaviour escalating?

Early signs can be subtle. Listening for context and change is often more important than waiting for obvious evidence of harm.

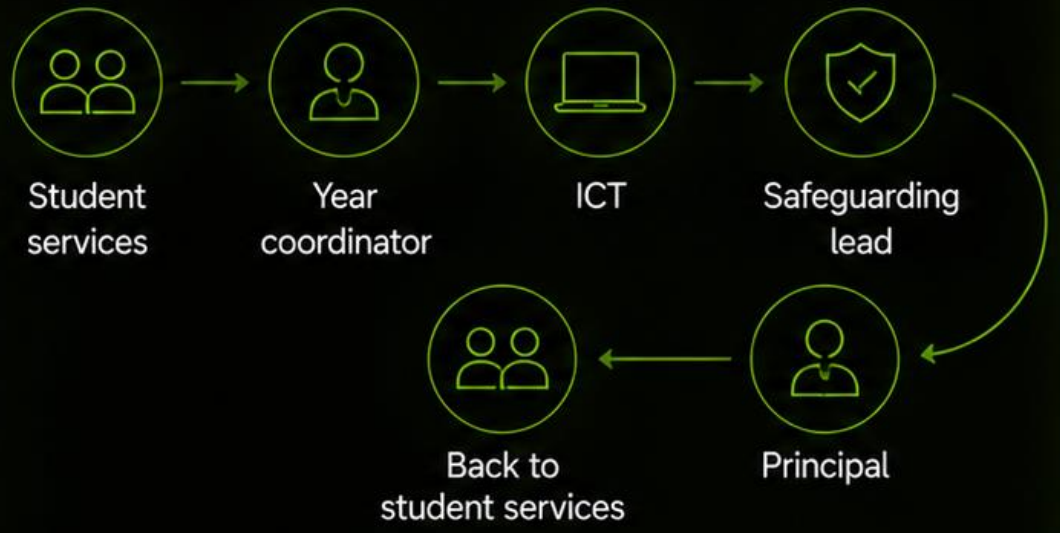
Concern may be recognised, but turning concern into action is complicated.

Cybernetic Shield

Action is delayed because:

- Behaviour appears low-level in isolation
- Intent is unclear
- Students minimise what happened
- Evidence is fragmented or changing
- The issue crosses several school functions
- Responsibility is unclear
- Staff are waiting for a recognised incident threshold

The common internal movement:



Every person may be acting reasonably,
but the **cumulative delay** can allow the incident to develop.

Early, proportionate action is not about overreacting.
It is about responding while the situation is still manageable.

Where responsibility blurs.

Online incidents often sit across school and home. Both environments matter.

School focus	Shared grey area	Parent focus
Student safety	Happens after hours	Device supervision
Wellbeing	Uses personal devices	Home boundaries
Learning and attendance	Begins privately	Monitoring activity
Peer relationships	Escalates socially	Platform understanding
School culture	Causes distress at school	Responding at home

Avoid presenting school and parent responsibilities as competing.

The practical position is often:

Parents manage the **home environment** and **device access.**

Schools manage **student safety** and the effect on **school participation.**

Both may need to **share information** and **coordinate action.**

Responsibility can be **shared** without the school assuming responsibility for everything that occurs online.

Cybernetic Shield

The focus shift.

Cybernetic Shield

Move from:	To:
“Did it happen at school?”	“What **impact** is it having?”
“Is it serious enough yet?”	“What suggests it may be **escalating**?”
“Which policy category does it fit?”	“What **support** or **protection** is needed now?”
	“What can we **safely** do while we establish more?”

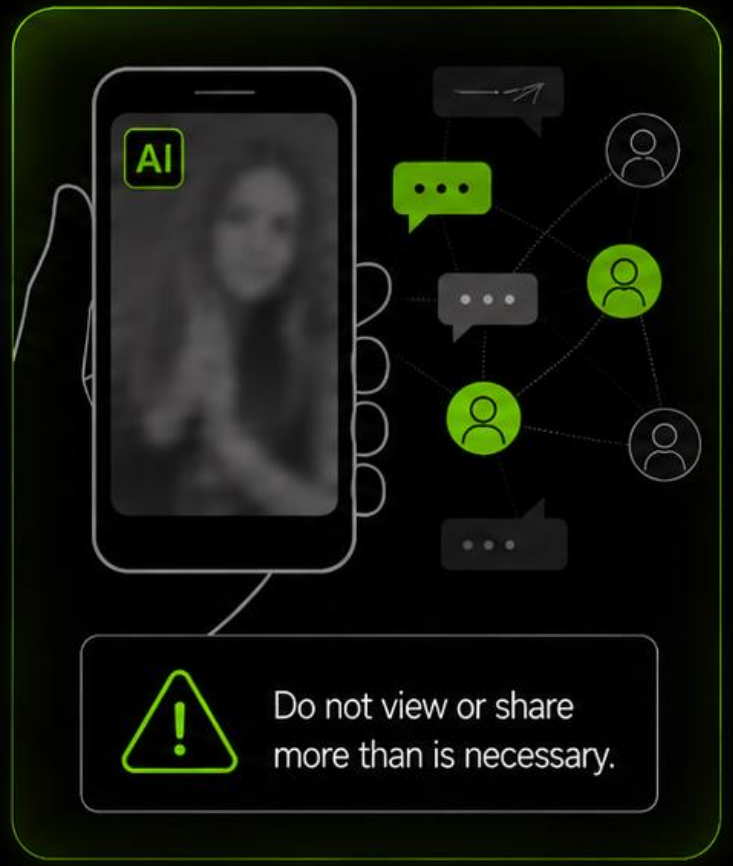
Cybernetic Shield

“It was only an AI joke”

A Year 9 student reports that another student has created an AI-generated sexualised image using her face.
It was first posted in a private group chat and has now been shown to other students.
The alleged creator says it was obviously fake and intended as a joke.

Key issues

- Sexualised content
- Lack of consent
- Possible image-based abuse
- Rapid redistribution
- Humiliation and reputational harm
- Possession and sharing concerns
- Need to avoid unnecessarily reproducing the material
- Potential safeguarding and law-enforcement considerations



Safe initial actions

- Support and stabilise the affected student
- Establish whether the content is still circulating
- Preserve limited, necessary evidence
- Do not ask multiple staff to view or forward it
- Separate containment from disciplinary investigation
- Escalate internally and seek specialist advice

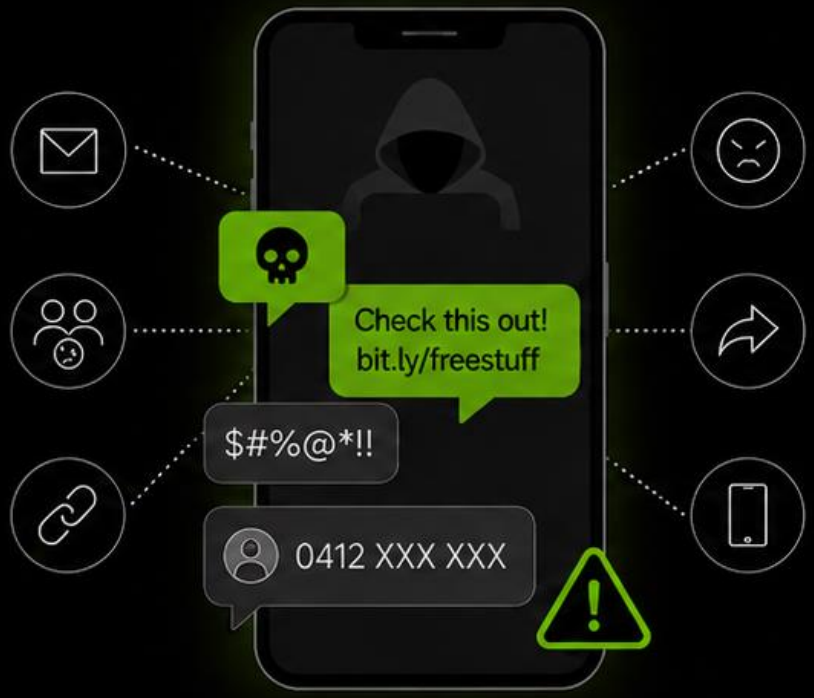
“Is this a safeguarding issue or an ICT issue?”

Cybernetic Shield

A student’s social media account is compromised. The attacker posts scam links, sends abusive messages to classmates and publishes the student’s phone number. Other students begin blaming the account holder for the messages.

Risks present

- Account compromise
- Impersonation
- Doxing (publication of personal information)
- Peer conflict
- Reputational harm
- Scam exposure
- Emotional distress
- Potential access to other linked accounts



Safe initial actions

- Secure the affected accounts and email
- Preserve evidence before content disappears
- Identify whether credentials were reused
- Alert likely recipients without unnecessarily repeating the content
- Document what was sent by the attacker
- Support the student with peer and reputational consequences
- Consider whether other students have clicked links or transferred money

This scenario demonstrates why online safeguarding and cybersecurity cannot always be separated. **The incident affects safety, wellbeing, reputation and digital security at the same time.**

What schools can safely do first

Cybernetic Shield

The **first response** does not need to solve the **whole incident.**

It should:

1	**Protect immediate safety and wellbeing**
2	**Preserve proportionate evidence**
3	**Reduce further spread or contact**
4	**Identify immediate escalation indicators**
5	**Coordinate who is leading the response**
6	**Record decisions and outstanding actions**

Useful questions in the first hour

- Is anyone in immediate danger?
- Is the behaviour continuing?
- Does another person have access to the child?
- Is content actively spreading?
- Are threats, coercion or demands involved?
- Is the student showing panic, withdrawal or acute distress?
- Does the school have enough evidence to seek help without gathering more harmful material?

The first hour should focus on stabilisation and containment, not an exhaustive interrogation.

What not to do.

Cybernetic Shield

Avoid:

- Asking the student to repeat the story to multiple adults
- Blaming them for sending, clicking or responding
- Forwarding harmful material unnecessarily
- Immediately deleting everything before evidence is preserved
- Promising complete confidentiality
- Contacting the alleged offender impulsively
- Treating containment and investigation as the same task
- Assuming an incident is resolved because content has been deleted
- Waiting for perfect certainty before providing support

Do not create additional copies of intimate or harmful material **simply to prove that it exists.**

Extra copies increase harm, risk and legal exposure.
Only capture what is necessary, and only by trained staff.

Cybernetic Shield

Online harm does not wait while adults decide.

Delayed or inconsistent responses can affect more than the original incident.

The incident

- greater spread
- stronger coercion
- more participants
- harder containment

The child

- panic, shame and anxiety
- school avoidance
- loss of trust
- reduced help-seeking

The school community

- harmful conduct becomes normalised
- reporting confidence falls
- boundaries become unclear

The organisation

- reactive crisis management
- staff uncertainty and workload
- complaints and parent escalation
- reputational impact

The value is early, calm and proportionate action.

What consistent real-time response looks like

Schools that respond well have clarity, confidence and consistency when concerns emerge.

> Do not wait for certainty. Look for indicators of escalation and focus on what the child needs now.

Cybernetic Shield

When the situation needs to be escalated

Seek additional support when there is:

Escalation indicators

- Immediate danger or serious distress
- Sexualised content involving a child
- Coercion, threats or extortion
- Suspected grooming or adult involvement
- Ongoing access to the student
- Rapid or uncontrolled content distribution
- Significant account or identity compromise
- Credible threats of harm
- Uncertainty about evidence, reporting or legal obligations
- A situation crossing several areas of school responsibility

Possible escalation pathways

- School safeguarding and executive leads
- Parents or carers
- Police or ReportCyber
- eSafety reporting and removal pathways
- Platform reporting
- Specialist incident-response support
- Psychological or crisis support

Cybernetic Shield

Escalation must be matched to the risk, circumstances and applicable reporting requirements.

Cybernetic Shield

When you need help

Different situations may need different support pathways.

Immediate danger

- Call 000
- Immediate risk to life or safety
- Urgent threat of harm or acute distress

Online abuse or harmful content

- eSafety
- Report image-based abuse, serious cyberbullying, sextortion or online abuse
- Use reporting and content-removal pathways where relevant

Cybercrime, scams or account compromise

- ReportCyber
- Scams, fraud, hacking, impersonation or account compromise
- Useful when a crime or cyber incident may have occurred

School support and next steps

- Cybernetic Shield
- Practical guidance on school response, evidence, containment and escalation
- Support for schools navigating complex online incidents

More than one pathway may be appropriate. Start with immediate safety, then choose the support that best fits the situation.

Five practical actions for schools

Cybernetic Shield

1. 

Define escalation indicators
secrecy, threats, rapid spread, coercion, distress and repeated targeting

2. 

Make responsibility visible
know who leads, who supports and who decides

3. 

Separate containment from investigation
protect the student while facts are still being established

4. 

Create a simple evidence process
screenshots, timestamps, URLs, usernames, disclosures and an audit trail

5. 

Rehearse realistic scenarios
AI images, sextortion, impersonation, account compromise and viral humiliation

Confidence comes from preparation, not improvisation under pressure.

Three things to take away

Cybernetic Shield

1

Online safeguarding is broader than cyberbullying.

The incident may involve safeguarding, wellbeing, technology, privacy and harmful behaviour simultaneously.

2

You do not need certainty to provide support.

Respond to indicators, patterns, progression and impact.

3

Early escalation is not an overreaction.

It creates visibility, coordination and protection while the situation is still manageable.

The aim is not for every educator to become an investigator or technology expert. It is for them to recognise when something may be developing, take safe initial action and know where to access help.

Thank you

Jessica Sears

jess@cyberneticshield.au

The aim is not for every educator to become an investigator or technology expert. It is to recognise when something may be developing, take safe initial action and know where to access help.

Questions?

Support is available through 4Cs and our incident support services.

Cybernetic Shield