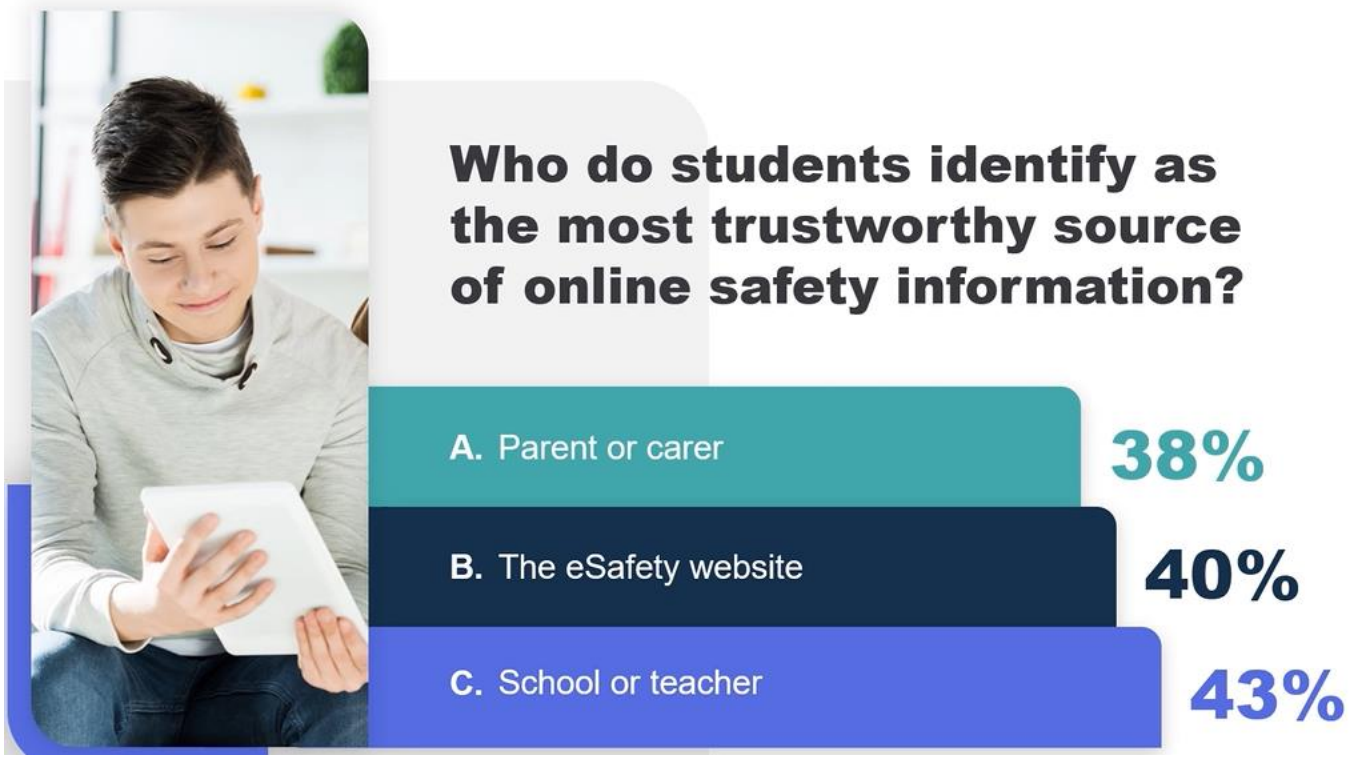
NSW Department of Education

Reporting Online Conduct Policy

Overview

Waterfall Public School (WPS) is committed to ensuring the wellbeing and holistic development of our students. WPS places student wellbeing as the highest priority. Research shows that students will often disclose online safety information to their teacher or school more often than their parents or the eSafety Commissioners website. It is therefore essential that we have a policy in place to support and guide our support services and responses to students.



This policy outlines the processes and procedures in place to effectively manage and report online conduct. This policy should be read in consultation with the Responding and Reporting eSafety Commissioner information and the Anti-Bullying Policy.

The Waterfall Way

The Waterfall Way informs our wellbeing programs with our school wide expectations:

- Be Safe
- Be Respectful
- Be an active learner

These values are promoted through explicit teaching, attendance tokens and learning tokens which contribute to merit certificates and Principal certificates.

Behaviour Code for Students

NSW public schools are committed to providing safe, supportive and responsive learning environments for everyone. We teach and model the behaviours we value in our students.

The Behaviour Code for Students is translated into multiple languages. At the start of each year and each term, students are explicitly taught the Behaviour code for students to ensure they understand what is expected and to support restorative conversations if required. Student reflection sheets are used by staff, during a teacher-student conference, to help students understand and adjust inappropriate behaviour. These are scanned and recorded in School Bytes, and attached to the student's file.

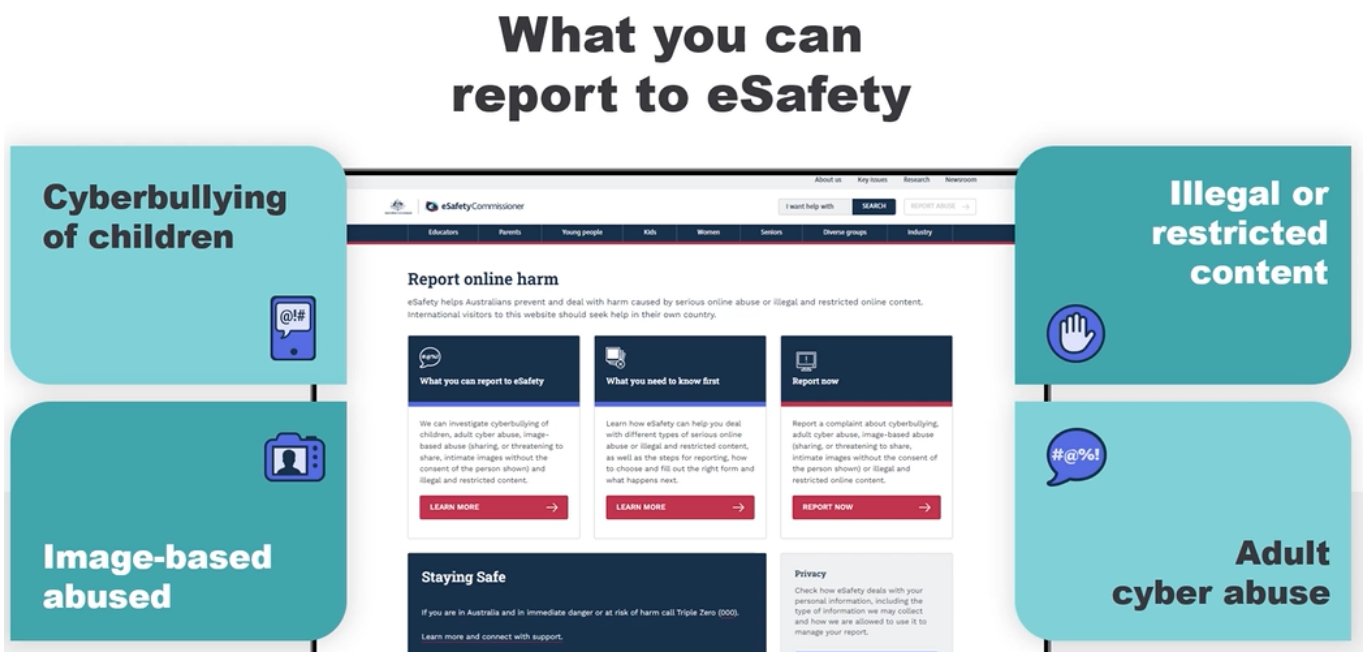
Explicit Teaching

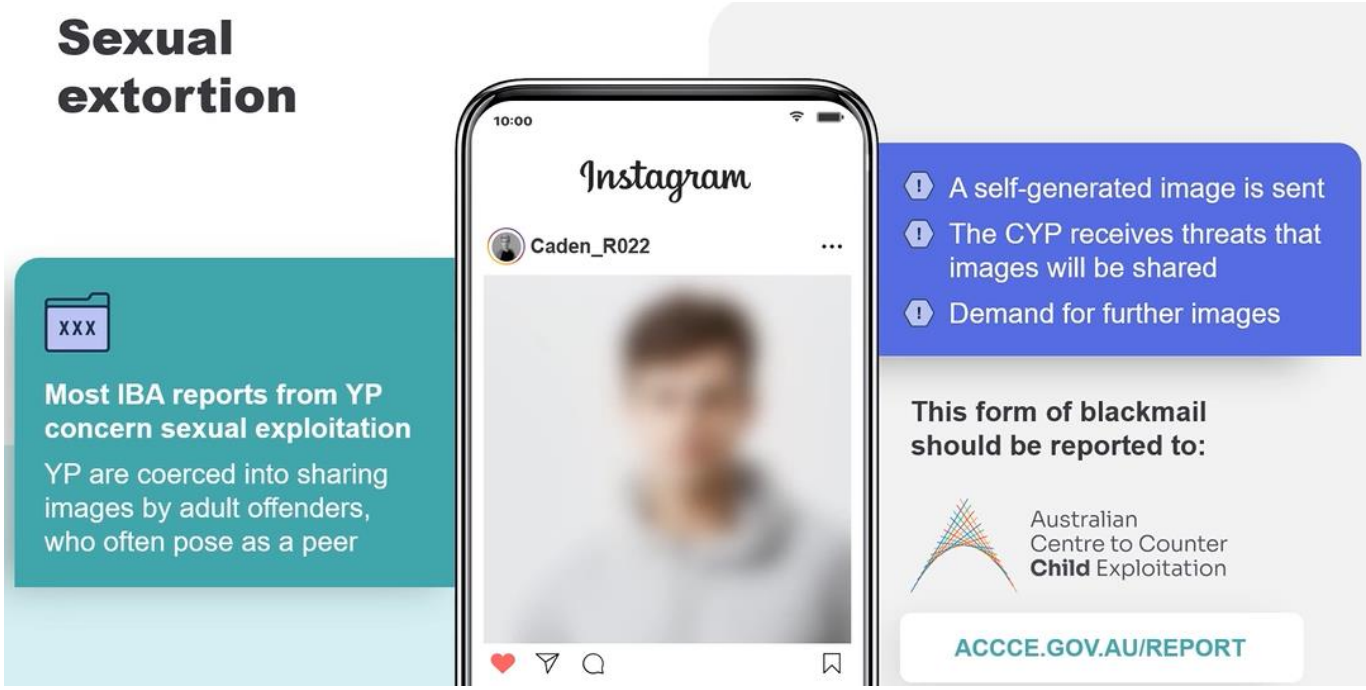
Each term, and as needed, K-6 students engage in eSafety lessons specifically aimed at ensuring the students know what is expected of them online, and how they can respond if someone is inappropriate online. The lessons come directly from the eSafety Commissioners website. In addition, throughout the year, students engage in virtual classroom lessons, run by the eSafety Commissioner, where they actively participate in lessons aimed at informing and supporting them.

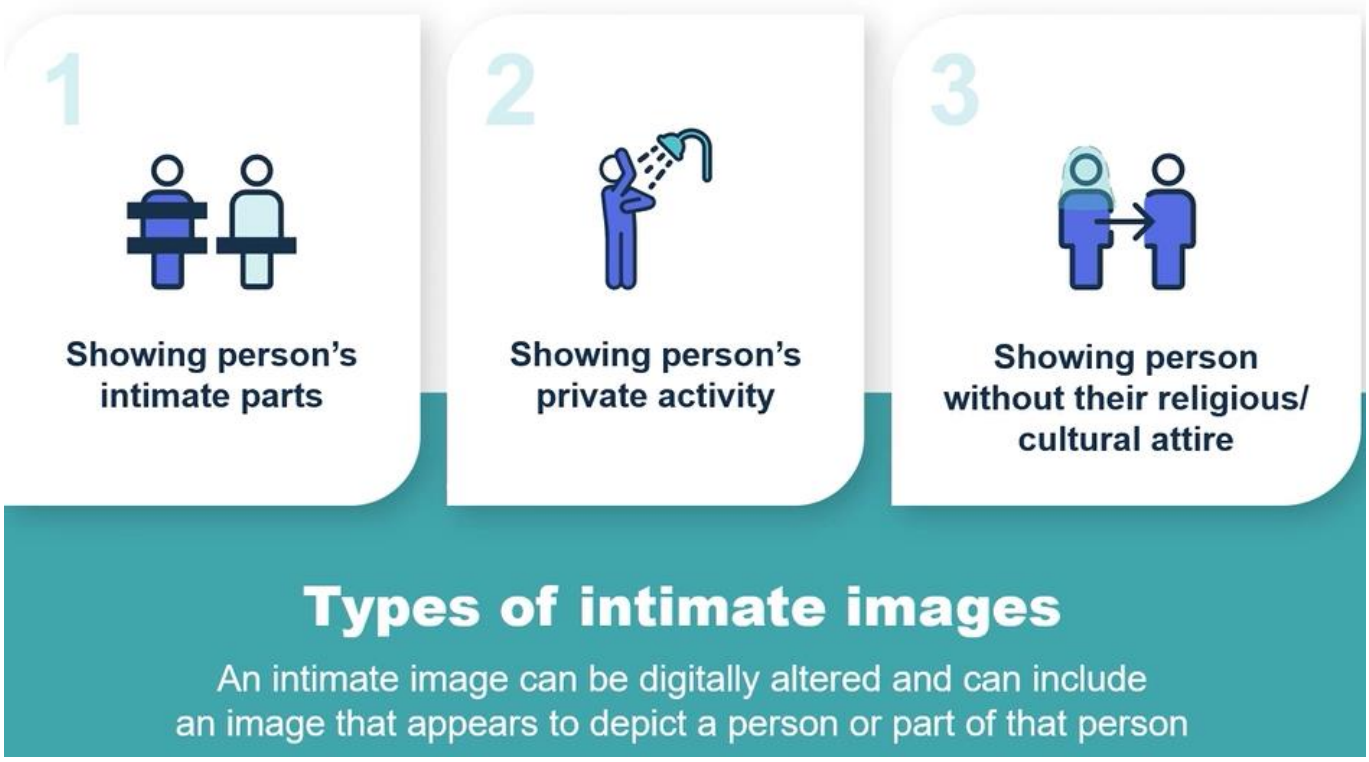
The eSafety Commissioner can investigate cases of serious cyber bullying if the service or platform does not respond tot eh initial complaint after 48 hours. The eSafety Commissioner also investigates illegal or restricted online content and adult cyber abuse.

Online Incidents

Esafety helps people to report abuse and get harmful online content removed. Cyber bulling and image-based abuse (sharing intimate images or videos without consent) are two types of abuse that can happen in a school setting. Content may be shared as a post, text image or video on a social media platform or online game.


What you can report to eSafety
Cyberbullying of children
Illegal or restricted content
Image-based abused
Adult cyber abuse
eSafetyCommissioner
Report online harm
What you can report to eSafety
What you need to know first
Report now
Staying Safe
Privacy


Sexual extortion
Most IBA reports from YP concern sexual exploitation
YP are coerced into sharing images by adult offenders, who often pose as a peer
10:00
Instagram
Caden_R022
A self-generated image is sent
The CYP receives threats that images will be shared
Demand for further images
This form of blackmail should be reported to:
Australian Centre to Counter Child Exploitation
ACCCE.GOV.AU/REPORT

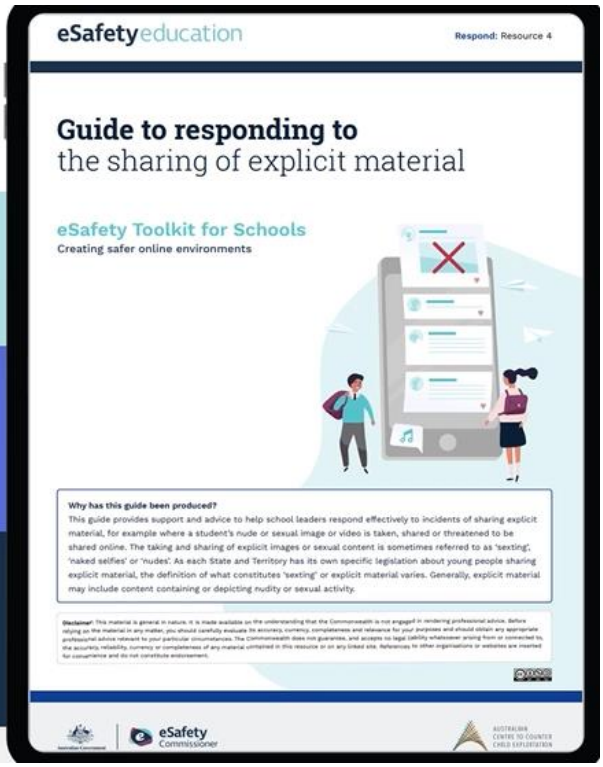


Reporting image-based abuse

An IBA threat or content does not need to be reported to the service first

Do not view, collect, print, share or store explicit material. **Make a written description and note where it is located**

Contact your Youth Liaison Officer or local Police and report to eSafety for advice on removal and online safety



Reporting fight videos or accounts

Encourage all involved to first report to the platform

Report to eSafety through the cyberbullying report form if not removed in 48 hours

To report to eSafety you must request the child's consent to report

This may be a child directly involved or another child who needs your support as the feel targeted or impacted

Self-harm and suicide

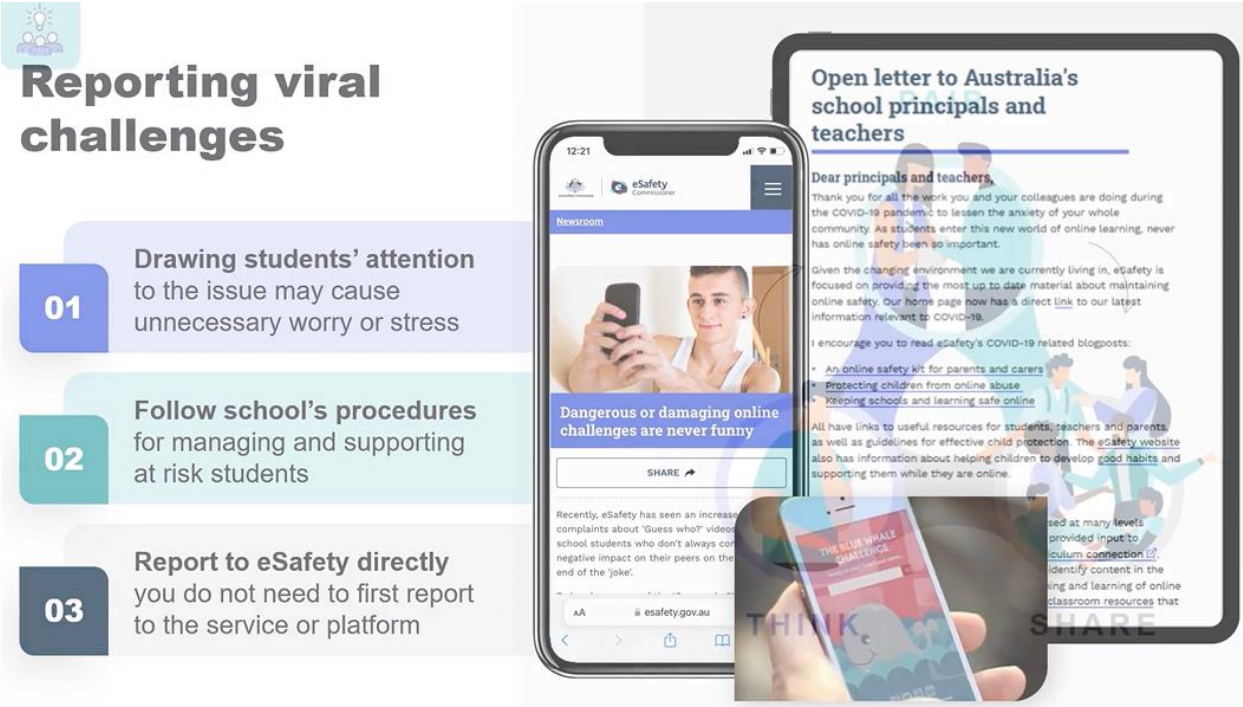
Report to **both** the platform and to eSafety

We can remove content that incites, instructs, or provides graphic depiction of self-harm or suicide

The content must be illegal or restricted and not just upsetting

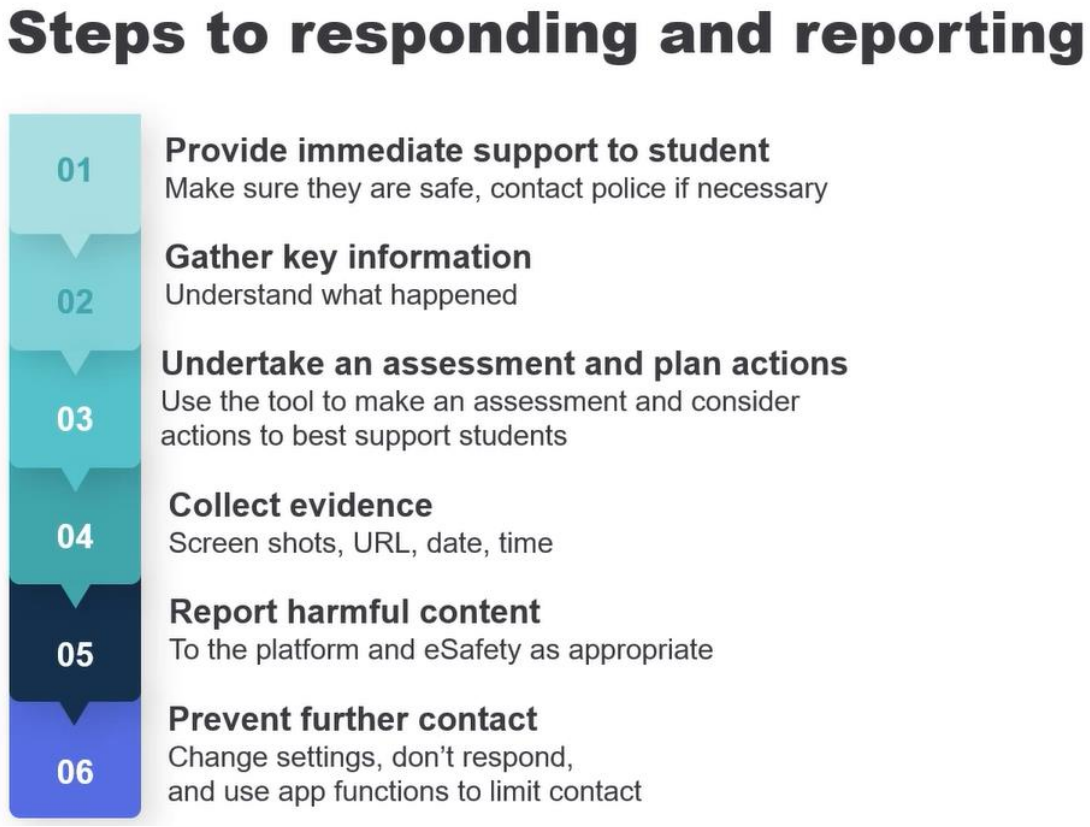
eSafetyCommissioner headspace

eSafety and headspace may communicate where there are concerns about this type of material



Steps to responding and reporting

Staff who are made aware of inappropriate online behaviour need to follow the steps below, in conjunction with the [eSafety quick reference guide] to help manage Online safety incidents.

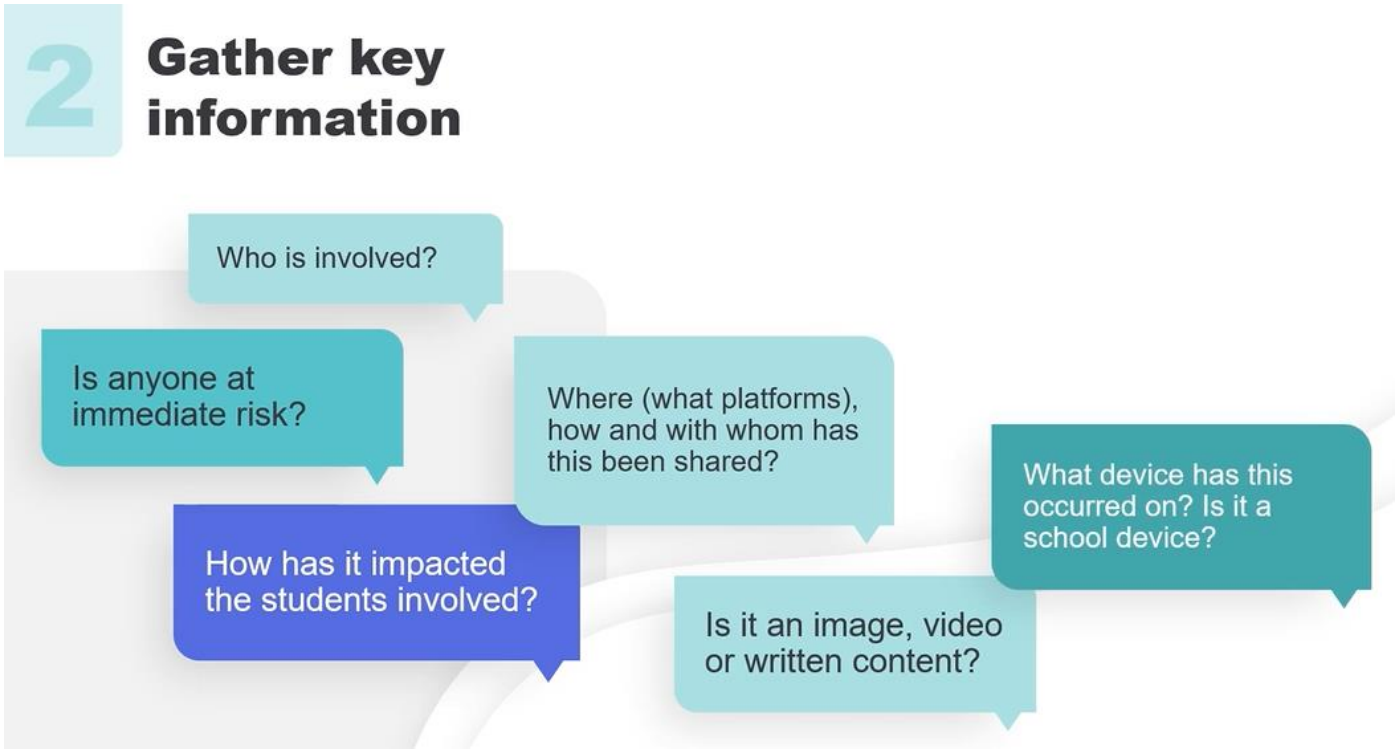


Step 1: Offer Support and Ensure Safety

Who: All staff members are responsible for offering support and ensuring safety.

Whenever a student's wellbeing is affected, we need to offer support and make sure they are safe. This can be provided in the classroom, year group, playground or other settings. At times, it may be necessary to employ the services of 'Team around a School', the school counsellor or other external agencies and providers to support the student. How we respond to a student when they are reporting bullying behaviour is critical. As a staff member, we need to remember how hard it might have been for the student to speak up and get help for themselves or their friend. It is essential to offer support and ensure safety by informing the class teacher and Principal of the wellbeing concern.

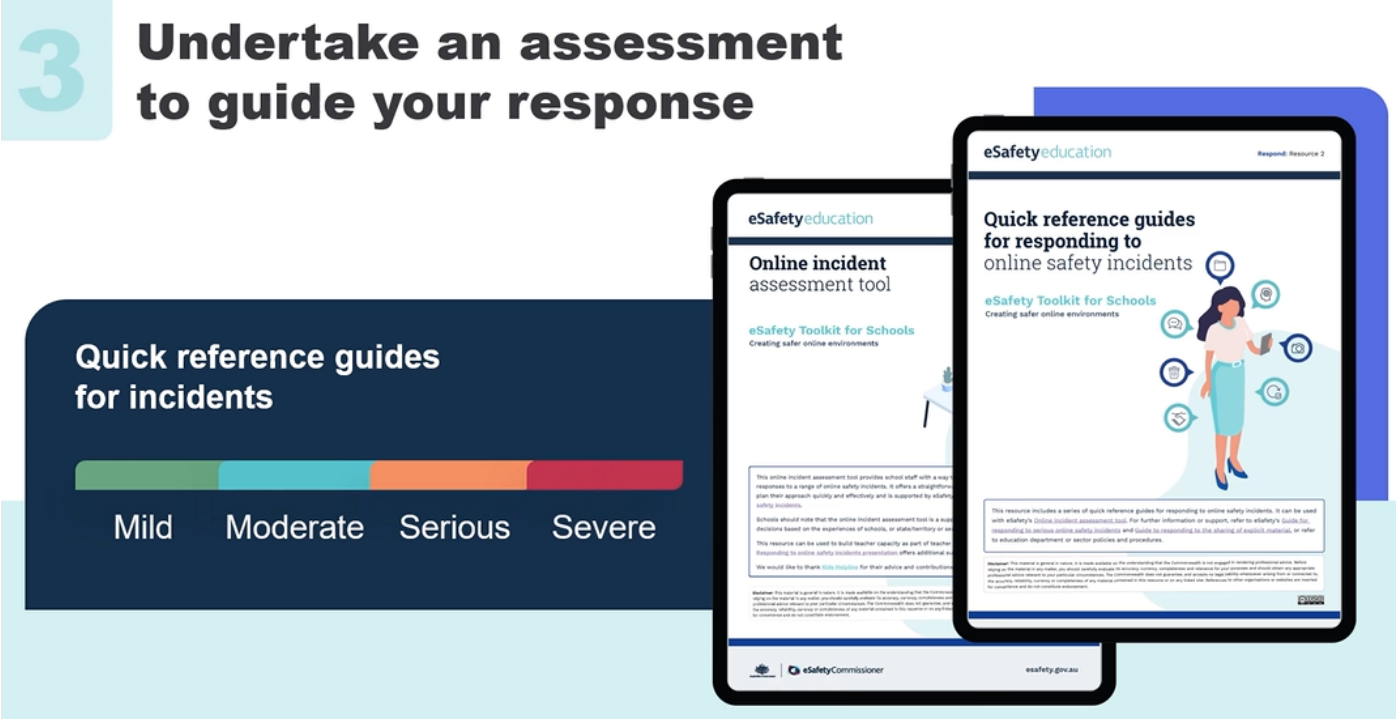
Step 2: Gather key information



Who: Class Teacher and Principal are responsible for gathering information.

It is essential to gather enough information to support the student, make an assessment and create a plan. This is a good time to document all other information that might influence the assessment, including the student's background, mental health and wellbeing history. It is essential not to conduct formal interviews or take official statements as this may form part of a police investigation if required. The situation may also become a child protection matter.

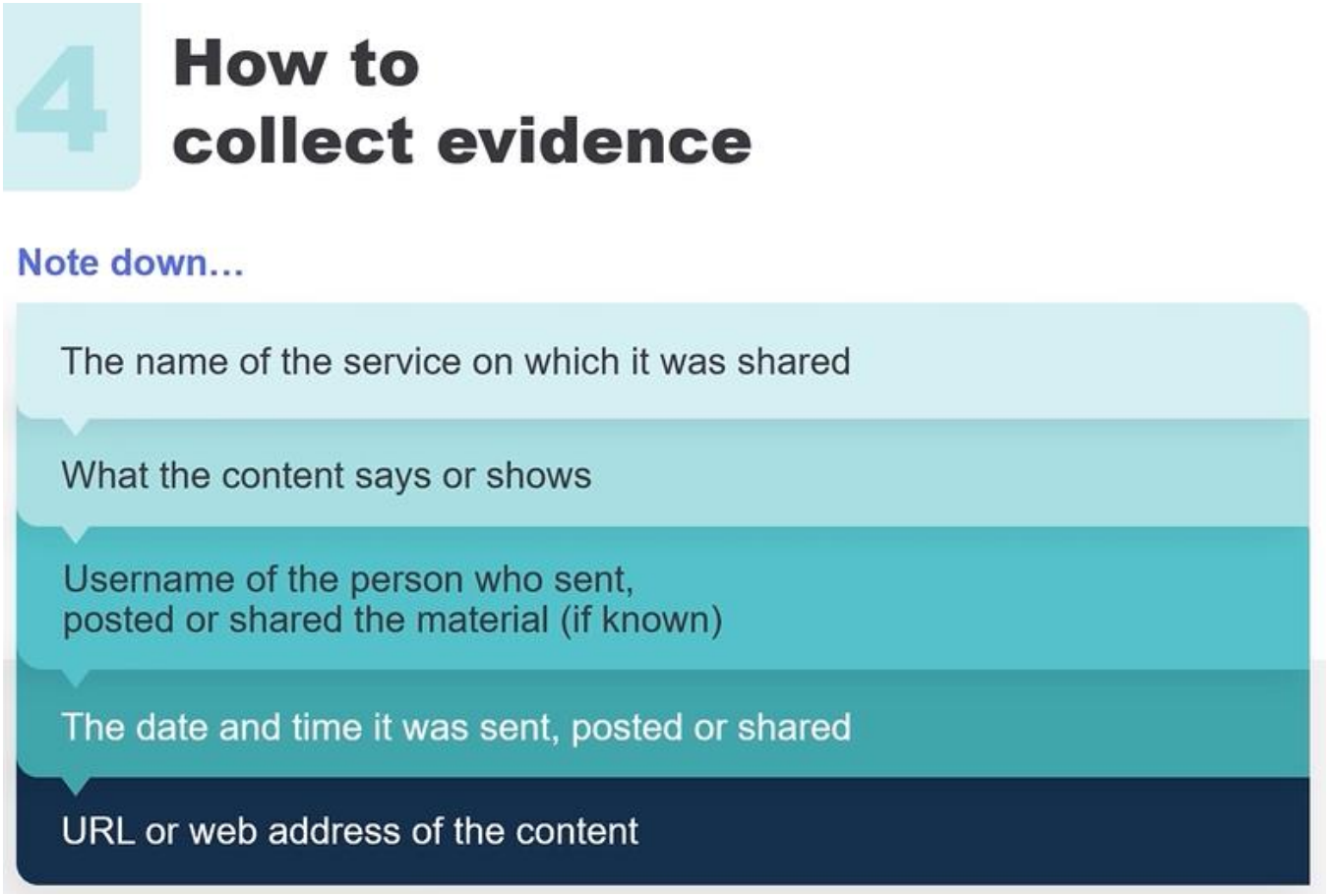
Step 3: Undertake an assessment and plan actions



Who: Class Teacher and Principal are responsible for undertaking an assessment and planning actions.

The eSafety Commissioner resources from the toolkit for schools can help determine the severity of an incident and suggest the planned actions. There are four incident ratings mild, moderate, serious and severe. Once planned actions have been determined, the response plan should be shared with any staff member who will have a role to play.

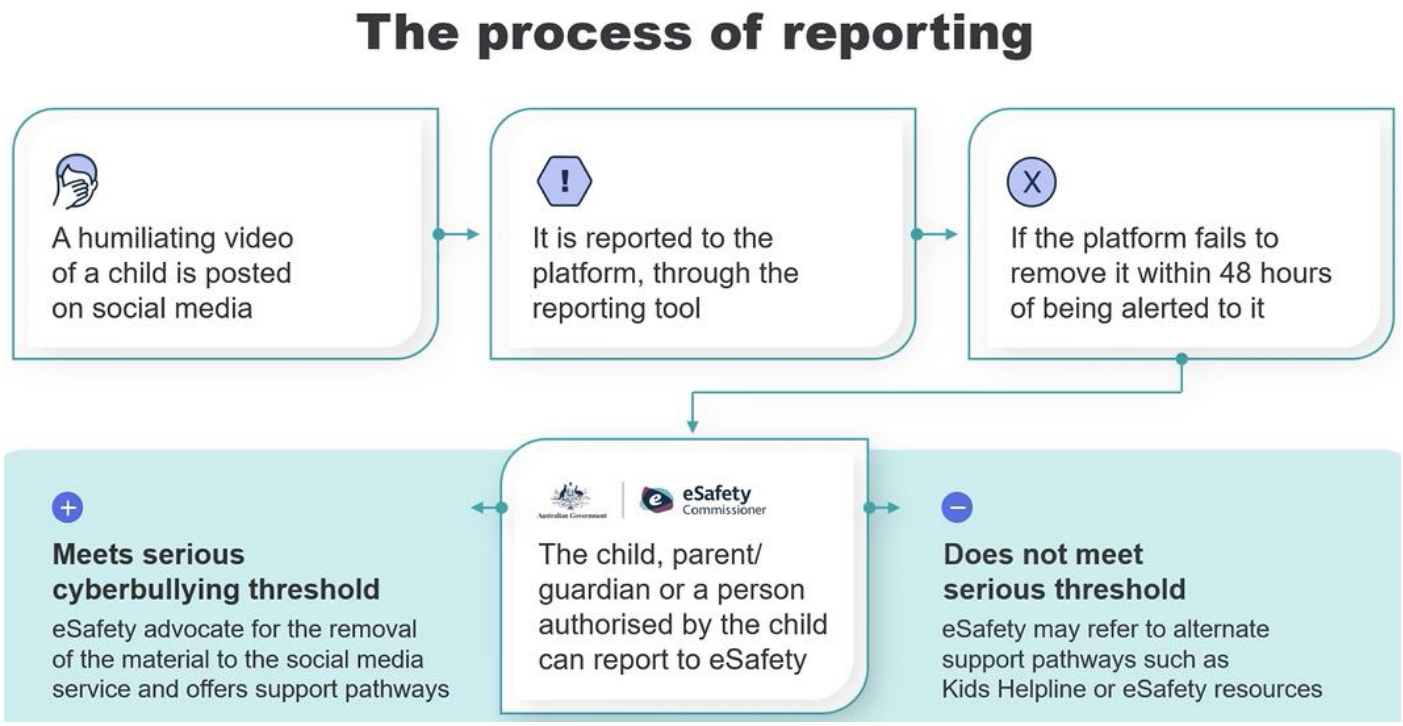
Step 4: Collect Evidence



Who: The Class Teacher and Principal are responsible for collecting evidence.

This step is essential if a report to the social media company or to the eSafety Commission is to be made. During this step, it is illegal to gather material, such as intimate images of a young person or material showing the exploitation of children. Do not print or save any copies of the information. The Principal will seek legal advice (ph:78143896) for the collection of evidence.

Step 5: Report Harmful Content



Who: All staff members are responsible for reporting harmful content. Any parent, student or guardian, or any adult authorised by the student can make a report to the eSafety Commissioner.

The most common type of online incident in Primary school is cyber bullying. This can be reported to the eSafety Commissioner once it is reported to the social media service. If the social media platform does not remove the content within 48 hours and it meets the legal threshold the eSafety Commissioner can help to have it taken down.

Any parent, student or guardian, or any adult *authorised by the student* can make a report to the eSafety Commissioner. This can include another teacher or trusted adult. The eSafety Commissioner investigation team will assess the report and take action, including supporting the student through the Kids Helpline or eSafety Resources.

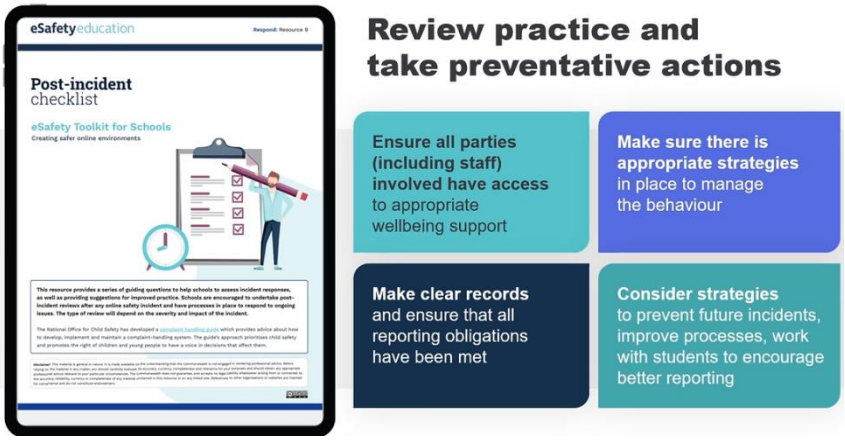
Step 6: Prevent further contact

Who: The parent or guardian is responsible for preventing further online contact.

This can be accomplished by changing passwords, changing settings, monitoring online interactions and not responding.

Review dates

Current review: Term 3 2024

Next review: Term 1 2025

Principal Name: Yvette Hopper