eSafety Policy

Australian schools are learning communities that promote student wellbeing, safety and positive relationships so that students can reach their full potential. The five interconnected elements of leadership, inclusion, student voice, partnerships and support provide the foundation for enhanced student wellbeing and learning outcomes."

Australian Student Wellbeing Framework 2018

Focus

Within an overarching **principle of inclusion**, there are seven minimum Standards that all schools must implement in line with Ministerial Order No 870. As educators, we have a mandatory obligation to create a culture which prioritises a safe, nurturing community for every child. The Standards provide a framework for routinely reviewing and strengthening child safety strategies, policies and practices. Ensuring the care, wellbeing and protection of children and young people in Catholic schools is inherent to the Catholic tradition which celebrates the sanctity and unique dignity of each human being.

At St. Anthony's Primary School we ensure we invest time and resources into raising a generation of smart, safe and responsible children who are capable and compassionate – both on and offline.

St. Anthony's Primary School has developed the eSmart policy using resources and information from the Victorian Department of Education and Early Childhood Development, Office for the eSafety Commissioner and through guidance from the eSmart program, an initiative of the Alannah and Madeline Foundation. The school has an Child Safety committee that has collaborated on developing this policy and procedures. Parents and students of the school community contributed and provided feedback on this policy.

Aim

This policy aims to provide a common understanding of cybersafety and cyberbullying in relation to the core values at St Anthony's Primary School. We believe in teaching online safety education that is empowering, builds resilience and effects positive social change, while also promoting the development of safe and appropriate long-term behaviours. Our current teaching practice, in line with the Victorian Curriculum, supports the development of digital literacy among teachers, parents and students.

St Anthony's Primary School takes into account the diversity of all students, including (but not limited to) the needs of Aboriginal students, students from culturally and/or linguistically diverse backgrounds, students with disabilities and students and young people who are vulnerable.

The policy outlines the staff, student and parent responsibilities required to ensure that the learning environment at St Anthony's Primary School is respected, valued and understood. Staff and Student User Agreements and Digital Working Statement have been developed in order to maintain the integrity of our school values.

Definition of common terms

Bullying

The national definition of bullying for Australian schools says;

Bullying is an ongoing and deliberate misuse of power in relationships through repeated verbal, physical and/or social behaviour that intends to cause physical, social and/or psychological harm. It can involve an individual or a group misusing their power, or perceived power, over one or more persons who feel unable to stop it from happening.

Bullying can happen in person or online, via various digital platforms and devices and it can be obvious (overt) or hidden (covert). Bullying behaviour is repeated, or has the potential to be repeated, over time (for example, through sharing of digital records).

Bullying of any form or for any reason can have immediate, medium and long-term effects on those involved, including bystanders. Single incidents and conflict or fights between equals, whether in person or online, are not defined as bullying. – Bullying. No Way! 2019

Types of Bullying

There are three types of bullying behaviour:

- ***Verbal bullying** which includes name calling or insulting someone about physical characteristics such as their weight or height, or other attributes including race, sexuality, culture, or religion*
- ***Physical bullying** which includes hitting or otherwise hurting someone, shoving or intimidating another person, or damaging or stealing their belongings*
- ***Social bullying** which includes consistently excluding another person or sharing information or images that will have a harmful effect on the other person.*

If any of these behaviours occur only once, or are part of a conflict between equals (no matter how inappropriate) they are not bullying. The behaviours alone don't define bullying.

Verbal, physical and social bullying can occur in person or online, directly or indirectly, overtly or covertly. - Bullying. No Way! 2019

Cyberbullying

The eSafety Commissioner’s website defines cyberbullying as:

“…the use of technology to bully someone — to deliberately and repeatedly engage in hostile behaviour to hurt them socially, psychologically or even physically. It is generally used to refer to the online abuse of children and young people. Groups and individuals can be both the perpetrators and targets of cyberbullying. Cyberbullying can take place on social media, through online chat and messaging services, text messages, emails, on message boards and in online forums that allow people to comment publicly.”

Cybersafety

The Enhancing Online Safety Act 2015 uses the following definition for cybersafety:

Online safety for children means the capacity of Australian children to use social media services and electronic services in a safe manner, and includes the protection of Australian children using those services from cyber-bullying material targeted at an Australian child.

Cyber-Risks

Cyber-risks are factors that contribute to or provide a platform for cyber-bullying or harm. These include unsupervised use of the internet, social media platforms, such as, Snapchat, Facebook, Instagram, Twitter and online marketing campaigns that promise prizes in return for personal details. Other cyber-risks include, stranger danger, inadvertently downloading viruses, hacking, insecure passwords and posting personal photos online. Tools, such as, firewalls, filters and anti-virus software may help reduce cyber-risks.

Principles

The use of digital technologies within our school by staff and students at St Anthony's is underpinned by the following principles and understanding:

- that digital technologies provide valuable opportunities for staff and students to collaborate, connect and create with peers, colleagues, experts and the wider community
- that online behaviour will at all times demonstrate respect for the dignity of each person in the community
- users will behave in a manner that is ethical when using the internet and network services (even for personal communication)

Curriculum

At St Anthony's Primary School, we ensure we invest time and resources into raising a generation of smart, safe and responsible children, who are capable and compassionate – both on and offline. The school has developed a wellbeing model based on the Australian Student Wellbeing Framework and EXCEL: Wellbeing for Learning, which emcompasses the intersecting dimensions of enable, connect, engage and learn. St. Anthony's Primary School has five core values that foster a safe, supportive and inclusive environment, allowing all students to flourish and experience success. St Anthony's uses appropriate cybersafety units from the Office of the eSafety Commissioner, and the Victorian Curriculum.

St Anthony's Primary School also participates in cross level teaching and promotion of cybersafety through Safer Internet Day, Harmony Day, National Day of Action Against Bullying and Violence, Day for Daniel and has a "buddy program" for Foundation and Senior students.

St Anthony's will provide instruction to students in online personal safety issues, including inappropriate sites, stranger danger, cyberbullying and scams. St Anthony's will prepare staff to deal with these issues.

Cyberbullying and bullying management process

Acceptable use and rules

Before using St Anthony's Primary School online resources, parents and guardians are asked to sign the Standard Collection Notice (G Suite for Education Parent Permission Form) sent out via Operoo at the start of each schooling year. G Suite for Education tools can be accessed at school, home, the library, or anywhere with Internet access.

St Anthony's Primary School has a Digital Literacy Outlines & Expectations policy (Appendix 4), a Student Acceptable Use Agreement (F-2), Student Acceptable Use Agreement (3-6), a Staff Acceptable Use Agreement, as well as, whole school Digital Working Statement (Appendix 5), which are taught at the beginning of the year and reinforced. The school has 5 school rules (Appendix 6) that cover all aspects of student safety and wellbeing.

Student Photograph / Video Policy

As of 2016, parents at St. Anthony's Primary School were asked to sign a "Photograph / Video Permission Form". Parents gave permission for their child's image to be used around the school and on the St. Anthony's Primary School website and social media platforms for their child's duration at St. Anthony's. Staff are informed and updated on any students whose parent did not give permission. At any time parents are able to request that their child's image not be used.

Student Mobile Phone and Devices Policy

Personal digital devices (mobile phones, iPads, gaming consoles, etc) are not to be brought to school unless a written note has been provided by parents and St Anthony's Primary School staff have given permission (Appendix 8). Students (who have permission) are required to drop their personal electronic devices at the office as soon as they enter the school grounds and pick them up at the conclusion of the day. Once handed in at the office, personal electronic devices will be stored in the office, with every care taken to ensure their security. Personal electronic devices brought to school are the sole responsibility of the student and no liability for lost, stolen or misplaced devices is accepted by St Anthony's Primary School.

Mobile phones are not to be used in the school yard, even prior to or after the school bell, this includes making calls, texting, using camera and internet functions, or using media/music players. They are only for contact with family organising to pick up their students at the conclusion of the school day following the bell. Videos or images of St Anthony Primary School's name, crest, staff and/or students are not to be stored on personal electronic devices or published on social media. Any student to be found to be in possession of a personal electronic device during school hours can expect to have the phone confiscated. It can be collected from the Office or Principal after school.

The use of any personal digital device at school events by students and/or parents is prohibited unless permission is granted by the School Principal.

Film Screening Policy

At times, teachers will for educational or entertainment purposes screen a movie or episode. St. Anthony's Primary School has a Roadshow Public Performance School Co-Curricular Licence. Teachers must only screen Australian Classification G rated movies / television episodes in Prep – Year 2. In Year 3-6, if for educational purposes only, a teacher wishes to screen a PG movie, the teacher must watch the movie beforehand in its entirety and seek parental permission for their child to watch that specific movie, outlining the types of themes covered in the movie / television episode.

Induction process

At St. Anthony's Primary School, it is the responsibility for the Classroom Teacher to induct any new students to the School Rules and Cybersafety rules. It is the responsibility of the Principal and the Induction Coordinator to induct any Casual Relief Staff, New Teaching Staff, Aides and other staff of the School's eSmart policy. A staff induction book outlining rules and policies is in the office for referral. The school will publish this policy along with the school rules on the school website: http: www.sameltonsth.catholic.edu.au

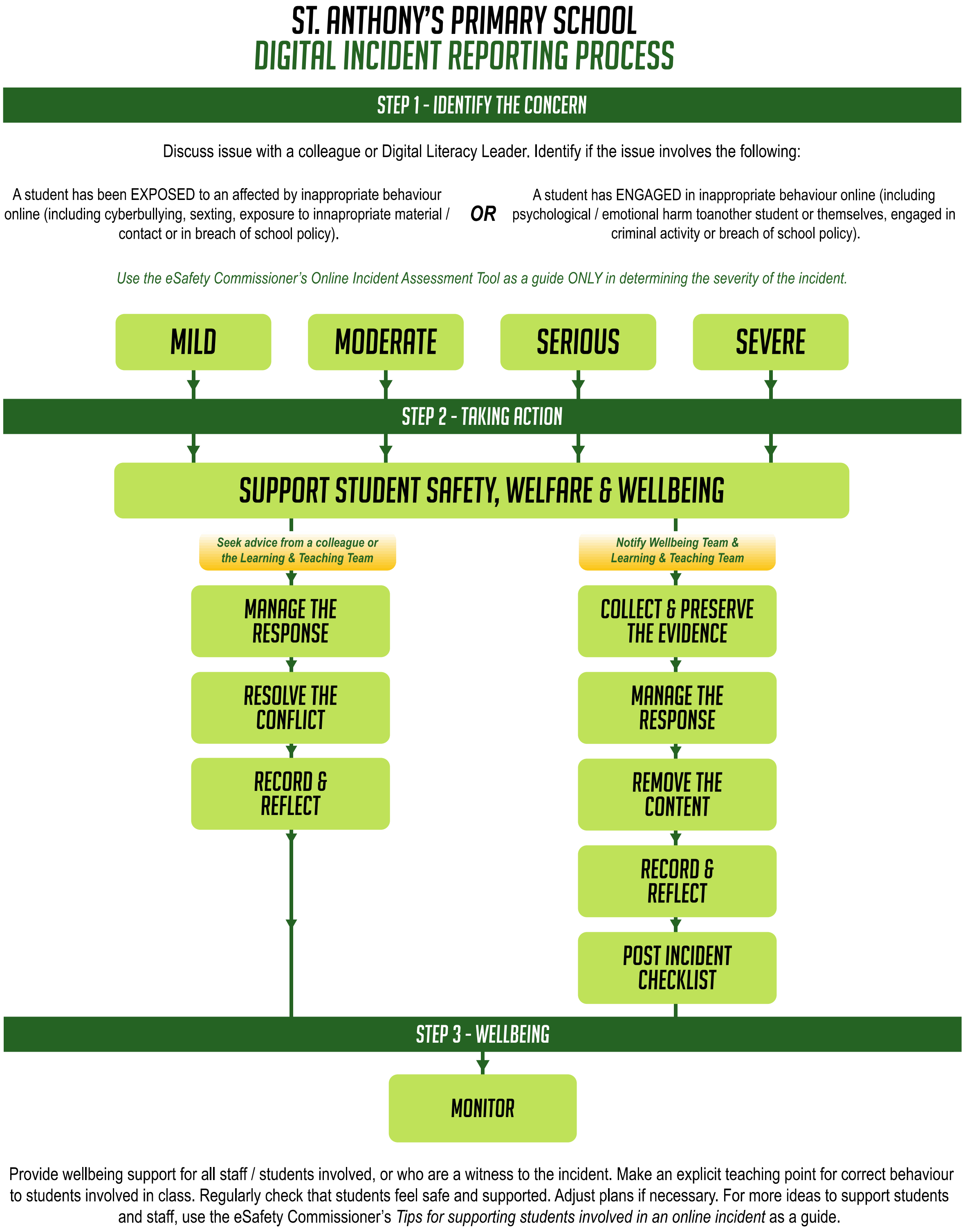
Important contacts

- Victoria Police (000)
- Kids Helpline (1800 55 1800 or www.kidshelpline.com.au)
- Headspace (1800 650 890 or www.headspace.org.au)
- eSafety: Make a Complaint (https://www.esafety.gov.au/report/cyberbullying
- Parentline (13 22 89 or www.education.vic.gov.au/parents/services-for-parents/Pages/parentline.aspx

References and links

- Australian Student Wellbeing Framework https://www.studentwellbeinghub.edu.au/educators/australian-student-wellbeing-framework#/
- Department of Education & Training https://www.education.gov.au/national-safe-schools-framework-0
- Office of the eSafety Commissioner www.esafety.gov.au
- Enhancing Online Safety Act 2015 https://www.legislation.gov.au/Details/C2018C00356
- Bullying. No Way! https://bullyingnoway.gov.au/
- Alannah & Madeline Foundation www.amf.org.au
- Australian Federal Police (AFP) www.afp.gov.au
- Smartcopying: The Official Guide to Copyright Issues for Australian Schools and TAFE www.smartcopying.edu.au
- Stay Smart Online www.staysmartonline.gov.au

Digital incident reporting checklist



ST. ANTHONY'S PRIMARY SCHOOL
DIGITAL INCIDENT REPORTING PROCESS

STEP 1 - IDENTIFY THE CONCERN

Discuss issue with a colleague or Digital Literacy Leader. Identify if the issue involves the following:

A student has been EXPOSED to an affected by inappropriate behaviour online (including cyberbullying, sexting, exposure to innapropriate material / contact or in breach of school policy).

OR

A student has ENGAGED in inappropriate behaviour online (including psychological / emotional harm toanother student or themselves, engaged in criminal activity or breach of school policy).

Use the eSafety Commissioner's Online Incident Assessment Tool as a guide ONLY in determining the severity of the incident.

MILD

MODERATE

SERIOUS

SEVERE

STEP 2 - TAKING ACTION

SUPPORT STUDENT SAFETY, WELFARE & WELLBEING

Seek advice from a colleague or the Learning & Teaching Team

MANAGE THE RESPONSE

RESOLVE THE CONFLICT

RECORD & REFLECT

Notify Wellbeing Team & Learning & Teaching Team

COLLECT & PRESERVE THE EVIDENCE

MANAGE THE RESPONSE

REMOVE THE CONTENT

RECORD & REFLECT

POST INCIDENT CHECKLIST

STEP 3 - WELLBEING

MONITOR

Provide wellbeing support for all staff / students involved, or who are a witness to the incident. Make an explicit teaching point for correct behaviour to students involved in class. Regularly check that students feel safe and supported. Adjust plans if necessary. For more ideas to support students and staff, use the eSafety Commissioner's *Tips for supporting students involved in an online incident* as a guide.

Outlines and Expectations

Appropriate use of resources

Digital Devices are wonderful tools that support engaging learning. The use of Digital Devices is a privilege, not a right, and inappropriate use could result in the loss of the privilege. The User Agreements at St. Anthony's Primary School applies to all devices that access the Internet and/or store information electronically.

Equipment

St Anthony's Primary School provides a variety of digital literacy tools for students to learn from. These include laptops, Chromebooks, iPads, robotics and more.

No food or drinks should be in the vicinity of any digital literacy equipment. All equipment should be handled with respect and care, they are not to be written on, to have stickers applied to them, or to be defaced in any way. Don't remove, move or write on the identification sticker on any digital literacy equipment.

iPads provided to Year 5 & 6 students must be in a student's possession or secured in a locked classroom in the recharge trolley at all times. They must not be lent to other students. iPads must be carried and transported appropriately on school grounds in their approved cases at all times.

Occupational Health and Safety

St Anthony Primary School encourages all users to read Tips for Laptop/iPad Users OH&S Policy.

Privacy

St Anthony's Primary School retains control, custody and supervision of all digital devices, networks and Internet services owned or leased by the school. The school reserves the right to monitor all digital devices and Internet activity by students and teachers. They should have no expectation of privacy in their use of school digital devices, Google Drive, email and stored files.

Damage

Vandalism or damage to Digital Devices, either deliberate or through neglect will result in cancellation of all privileges and the possibility of replacing damaged items. Vandalism is defined as any malicious attempt to harm or destroy equipment or data of another user, Primary School ICT hardware and software and computing rooms. This includes the transmission of computer viruses, theft of hardware and software.

Digital Citizenship

“Digital citizenship is about confident and positive engagement with digital technology.”

“A digital citizen is a person with the skills and knowledge to effectively use digital technologies to participate in society, communicate with others and create and consume digital content.” *Digital Citizenship, Office for the eSafety Commissioner*

St Anthony’s Primary School is dedicated to teaching and developing positive, appropriate and constructive online behaviour with our students. Students will be encouraged to navigate the online world safely by developing four critical skills outlined by the Office for the eSafety Commissioner;

- **Respect** - I treat myself and others the way I like to be treated
- **Responsibility** - I am accountable for my actions and I take a stand when I feel something is wrong
- **Reasoning** - I question what is real
- **Resilience** - I get back up from tough situations

Cybercrime

The Australian Federal Police (AFP) defines cybercrime as:

In Australia, the term ‘cybercrime’ is used to describe both:

- *Crimes directed at computers or other devices / information communications technologies (for example, hacking)*
- *Where computers or other devices / information communications technologies are an integral part of an offence (for example, online fraud, identity theft and the distribution of child exploitation material).*

Common types of cybercrime include cyberbullying, hacking, online scams and fraud, identity theft, attacks on computer systems and illegal or prohibited online content.

Australian defamation law dictates that a person is guilty of defamation when;

“A person who ‘publishes’ an assertion of fact or a comment that: injures - or, importantly, it ‘likely’ to injure - the personal, professional, trade or business reputation of an individual or a company: Exposes them to ridicule; or cause people to avoid them.”

St Anthony’s Primary School recognises that the majority of cybercrime cases occur outside of its controlled network. However, to ensure that students and parents are aware of cybercrime and the correct actions to take, this policy includes protection for its own name, crest, students and teachers.

In case of cybercrime affecting a student outside of the school boundaries, the following course of action should be take;

- The student immediately informs his/her parents/carers
- The student immediately informs the school
- The abuse is reported to the website owner or webmaster
- If the concern is considered serious then the police should be informed immediately

A case of cybercrime/defamation against St Anthony’s Primary School staff member or the Primary school occurs if;

- A video or image of St Anthony’s Primary School staff member is placed on a public website without the permission of the staff member
- Information about a staff member including their name is placed on a public website without the permission of the staff member
- The St Anthony’s Primary School name or crest is published on a public website without the written permission of the Principal

Protect your identity

St Anthony's Primary School will not tolerate students using digital devices to bully or harass others. Students found engaging in such activities will be dealt with in the strongest possible terms.

Cybersafety sessions will be conducted for students, staff and parents at the discretion of the school Digital Literacy Leaders.

Students should make every effort to protect their identity and the identity of the school through email and the Internet. That information includes name, age, address, phone number, photographs or parent's names. Identity theft is a growing problem and it is better to safeguard your information.

Protect your password

All students have been given a unique password linked with their personal username. Passwords are not to be shared with other people. If you are concerned about your privacy please speak with one of the Digital Technology Leaders. At no stage are you to use another individual's login and password.

Inappropriate material

Students will not use Digital Devices to access material that is inappropriate, profane or obscene that advocates illegal acts, or that advocates violence or discrimination towards other people. If a student mistakenly accesses inappropriate material, they should immediately inform the supervising teacher. This will protect the student against a claim that such access was intentional.

Copyright

Smartcopying: The Official Guide to Copyright Issues for Australian Schools and TAFE defines copyright as:

A simple definition of copyright is that it is a bunch of rights in certain creative works such as text, artistic works, music, computer programs, sound recordings and films. The rights are granted exclusively to the copyright owner to reproduce the material, and for some material, the right to perform or show the work to the public. Copyright owners can prevent others from reproducing or communicating their work without their permission or may sell these rights to someone else.

Copyright laws and licensing agreements must be respected and sources appropriately acknowledged. Users must not breach laws of copyright, moral right or intellectual property - this includes illegal copies of software, music, videos and images.

Students will respect the rights of copyright holders. Infringing copyright is illegal. Copyright infringement occurs when you inappropriately reproduce a work that is protected by copyright.

All material submitted for publication must be appropriate to the school environment and copyright laws.

Students must not copy data found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were your own. In completing tasks, references to such sources should be provided in the bibliography.

Copyright includes but is not limited to:

- Copying software owned by the Primary School or by using Primary School resources;
- Downloading software without direct approval of a staff member
- Copying images, clipart or art works
- Using Primary School ICT resources to obtain program cracks
- Installing software on laptops, Chromebooks or iPads
- Downloading or copying music from the internet

Social media

St Anthony's School accepts that the use of Social Media can be an effective business and social tool and that such media is commonly used to express views, comments, and ideas on a range of issues.

However, it is expected that all members of the St Anthony's community behave in such a manner that:

- The welfare of all members of the school is not adversely impacted upon.
- The reputation of the school is not negatively affected or brought into disrepute.

When using Social Media, it is expected that members of our school community will:

- Demonstrate appropriate personal and professional boundaries and behaviours.
- Ensure online behaviour reflects the same standards of honesty, respect, and consideration that a person uses when communicating face-to-face.
- Respect the rights, privacy and confidentiality of others.
- Ensure all content published is accurate and not misleading.
- Not post or respond to material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, threatening, violent, racist, sexist, pornographic, or is otherwise unlawful.
- Not infringe on copyright or cause damage to the reputation of St Anthony's school, or bring it into disrepute.

Staff will need to refer to the St. Anthony's Primary School Social Media Policy.

Storage of work

Students and teachers are responsible for the careful storage and backing up of their work.

St Anthony's Primary School accepts no responsibility for files lost or altered due to problems with our infrastructure or hardware. Hard drives or cloud storage (Google Drive) may be treated like school property in that staff may review files or communications to maintain system integrity and ensure that users are using the system responsibly. All users should not expect that files stored on their Google Drive are private.

Email

Email service is provided for educational and administrative purposes. Staff and students at St Anthony's must identify themselves appropriately by using a signature block at the bottom of the email message that includes their name, school phone number and postal address.

School email addresses are not to be given to ANY websites, companies, or other third parties with the exception of educational websites for staff. St Anthony's Primary School advises students and staff that they may be held accountable for the email they create and distribute using the network. School email addresses are to be used for school-related purposes only. Only school-related attachments may be sent on the school email system.

Settings for devices

School rules and the St Anthony's Primary School emblem are to be used only. Inappropriate or copyrighted media may not be used as a screensaver. iPad provided desktops and family photos or created images are encouraged. Presence of weapons, inappropriate images, inappropriate language, alcohol, drug, gang related symbols or pictures, will result in disciplinary action.

Do not change your name or settings in Google. St Anthony's Primary School has the right to suspend users who are not abiding by the rules.

Audio and video

Listening to music either aloud or with earphones is not permitted in class unless required for the activity being conducted or class teacher gives permission. When sound is needed, headphones, provided by the student, must be used. Any audio or video recording may be done only with the prior permission of all parties being recorded. Sharing of music (including iTunes music sharing) over the school network is strictly prohibited and is subject to appropriate consequences.

Games

Downloading, viewing and/or playing of electronic online games is not permitted except as part of an assigned, in-class activity. The school reserves the right to remove any game from a school digital device that is considered inappropriate or impedes the educational purpose of the lesson. Online games are not to be 'played' over the school network. Games that include violence, adult content, inappropriate language, and weapons are not to be installed or 'played' on school computers, including the iPads.

Chatrooms, messaging, news groups

Students are not permitted to use instant messaging or social networking on school equipment.

Internet use

Access to internet and network services are provided by MACS to staff and students of St Anthony's Primary School for educational and administrative purposes. From time to time, other MACS policies and requirements in particular schools may result in restrictions.

Access rights assigned to students and staff at St Anthony's Primary School will be determined by the principal and may vary as educational and administrative purposes change.

Students and staff at St Anthony's may not use the internet and network services provided for commercial purposes, either offering or acquiring goods or services for personal use. The services cannot be used for political lobbying or proliferation of unnecessary communications.

Network access

The utilization of proxy avoidance IP numbers and programs is strictly prohibited. Students may not use the school network for personal or private business reasons. Students are not to knowingly degrade or disrupt online services. This includes tampering with computer hardware or software, vandalizing data, installing computer viruses, attempting to gain access to restricted or unauthorised network services, or violating copyright laws. St Anthony's Primary School is not responsible for damaged or lost data transferred through our network or stored on laptops, computers or our file servers.

File sharing

File sharing is the public or private sharing of computer data or space. Any program that creates a point-to-point connection between two or more computer devices for the purpose of sharing data is considered file sharing. File sharing of any kind is prohibited both at school and at home. The only exception to this is when it is a specific assignment given by the teacher, using GAFE and Airdrop (iPads) for educational purposes only.

Downloading, loading and streaming software

All installed software must be a legally licensed copy and approved by St Anthony’s Primary School Digital Leaders. The downloading of music files, video files, games, etc. through the school's network is absolutely prohibited unless it is part of an assigned, in class activity. The school reserves the right to remove any software that has been loaded onto the digital device that impedes the educational purpose of the lesson. Only commercial videos (such as television programs) legally purchased from the iTunes music store or another like entity (ABC iView, etc) may be downloaded to the digital devices. To download apps, please request permission through the App Request Ticket.

Consequences

The school reserves the right to enforce appropriate consequences for the violation of any section of the Outlines & Expectations policy. Such consequences could include the loss of privileges of Digital Devices, the loss of the use of the Digital Device for an amount of time determined by the administration and members of the Technology Department, possible disciplinary action, and possible legal action. These consequences apply to all students and staff at St Anthony’s Primary School.

Digital Devices with illegal or inappropriate software or materials on them will be reformatted or “reimaged.” In the case of repeated Digital Device abuse and/or damages, the school has the right to revoke the use of the technology. Students and staff are to report any known violations of this Outlines & Expectations policy to appropriate administrative staff members.

Random checks of student digital devices will be conducted throughout the year to ensure that these policies are being followed. St Anthony’s Primary School takes no responsibility for activities conducted on school digital devices or materials stored on computers, laptops, iPads or the school's network. If you are unsure about the application of any of the above rules, check with your teacher or Digital Literacy Leader first.

Digital Working Statement

The school’s Digital Equipment are learning tools, to be used **FOR EDUCATION, NOT RECREATION**.

All Digital Equipment use should be **RESPECTFUL, APPROPRIATE, CONSTRUCTIVE AND POSITIVE**.

Student’s need their **TEACHER’S PERMISSION** before using any program, game, website etc.

Students need to be **RESPONSIBLE** for ensuring their Digital Equipment and accessories are handled **WITH CARE**.

Students **MUST REPORT ANY INAPPROPRIATE USE** as soon as they know about it.

TAKE A STAND AGAINST BULLYING and make sure that you are not bullied or that you do not bully others. Report all bullying to an adult.

ALWAYS make the right choice when using Digital Devices.

Using Digital Devices is a privilege, not a right!

CONSEQUENCES

1. Warning
2. Loss of iPad for a period of time determined by the teacher / school. Parents will be informed of inappropriate use.
3. Sent to the Principal. Followed by meeting with the parents.
4. Deactivation of email account.

Online Incident Assessment Tool

USING THIS RESOURCE

All online safety incidents need to be taken seriously and responded to appropriately, in line with the school's duty of care to students and staff. However, online safety incidents can vary in their severity and impact on the target. The following tool is designed to help schools assess the seriousness (mild, moderate, serious, or severe) of an incident and develop a suitable response.

Schools should also base any assessment on their knowledge of the student and the incident.

Remember to consider:

- A student's unique background and circumstances, any vulnerabilities and the relationship between the target   and the instigator. The relationships within, and between, these factors may be complex, for example targets and bystanders can also be instigators.
- That students may initially mask or downplay the impact of an incident. Schools should try to understand the circumstances surrounding an incident before assessing its severity.
- Consider the tone, impact and intent of the language, audio or visual content and any sensitivities. This includes where it has been shared and the number of times it has been shared or viewed.

Some incidents may involve unlawful behaviour, child abuse or adult perpetrators. Staff should not investigate these types of incidents independently. In the first instance, the incident and the most appropriate course of action should be discussed with the principal/school leadership team, accounting for students' rights and best interests. The Principal/school leadership team may consult with the child protection/student wellbeing officer in the school and engage local police or a relevant child protection agency.

INSTRUCTIONS

The following online incident assessment tool categorises and rates the severity of a range of online safety issues. It can help staff to determine an overall incident rating, accounting for the frequency and impact of the incident, and types of behaviour displayed. School staff can use this assessment to underpin the school's response.

In using the tool, staff should choose one option from each category that best reflects the incident. If the incident fits two options, pick the option with the highest rating.

Each option has been allocated a rating. Once an option has been chosen from each category, and the rating confirmed, these ratings can be added together to form a combined overall rating. This overall rating has a corresponding recommended course of action. Remember that while the recommended actions support schools to respond to an incident but more targeted actions may be required due to the specific circumstances of the incident.

The overall ratings, and related responses, are:

- Severe = Overall rating 8-9
- Serious = Overall rating 6-7
- Moderate = Overall rating 4-5
- Mild = Overall rating 1-3

IMPORTANT NOTE

- Call Triple 000 if a student is at risk of immediate harm.
- If any individual category has been scored a 3, rate the incident as Serious at a minimum.
- An initial assessment may change (e.g. Moderate to Serious) as new information is received.
- School staff may decide to assess an incident as Serious or Severe for reasons other than those stated.
- When considering the broader circumstances surrounding the issue, remember that student vulnerability may be influenced by factors such as mental health, disability, or lack of social or familial support.

This tool is intended as a guide only.
It should be adapted to each online safety incident and the individuals involved.

Behaviour	Description	Rating
Teasing, name calling, put downs	General name calling or swearing. Does not include 'hate speech' or name calling based on discrimination (see hate speech, below).	1
Meme posts	Memes (pictures/videos with accompanying text) that are designed to make fun of someone, usually as a joke.	1
Social exclusion	Deleting students from group chats, excluding students from private groups, photoshopping an individual from images, excluding players from online games.	1
Impersonation and meme accounts	Creating fake social media profiles for someone, using fake accounts to cause friendship or relationship issues, misrepresenting someone online, creating accounts dedicated to sharing hurtful memes.	2
Fighting accounts/ sharing violent images or videos	Accounts that include videos of students fighting or engaging in physical bullying, sharing violent images and videos.	2
Sharing inappropriate sexualised messages	Rating or polling someone's attractiveness, sending explicit text messages.	2
Unwanted or uncomfortable contact	Student contacted by an unknown person, for an unknown reason. The contact tries to persuade the student to participate in risky online behaviours such as scams, gambling or dares/challenges. There are no clear sexual connotations.	2
Hate speech, discrimination and sexual harassment	Targeting someone because of their personal identity/beliefs (e.g. race, ethnicity, sex/ gender, nationality, sexual orientation, religion, age, disability) or persistently making sexual advances.	3
Incitement to suicide or self- harm	Encouraging a student to self-harm or consider suicide (e.g. the world would be better without you in it) **Note:** if you become aware that a student has been posting on social media about suicide or self-harm, refer to your school's duty of care policy and consider seeking advice from local police or support services. Orygen's #chatsafe guidelines provide information about how to respond.	3
Threats of physical harm	Threatening to physically hurt someone — such as written threats, posting fight videos with threats of retaliation or posting photos with images to suggest harm will be inflicted.	3
Non-consensual sharing of intimate images	Sharing intimate (naked/sexual/private) images or videos without the consent of the person in the image. Includes images/videos of people without attire of religious or cultural significance usually worn in public by the person in the image.	3
Online grooming	A deliberately established emotional connection with a child by someone online in order to lower their inhibitions and make it easier to have sexual contact with them. It may include adults posing as children in chat rooms or on social media sites to 'befriend' a child in order to meet with them in person. Grooming can include obtaining intimate images of young people.	3

Frequency **Important note** The frequency of an incident may not be evident on first appearance. A student may mask that an incident has occurred repeatedly, or over an extended time. Responses may need to be escalated or de-escalated depending on the situation or new information coming to hand.	**Rating**
• First time and instigator is likely to stop. • Is a contained incident between two people.	1
• Has happened occasionally. • Instigator continues after they have been asked to stop. • Has occurred on several platforms/mediums. • Has occurred as part of a friendship group situation.	2
• Has happened many times before. • Instigator unlikely to stop. • Is part of a wider situation involving a number of students/aprents/others?	3

Impact **Important note** The way that an incident impacts a student may not be static or obvious. Students may initially mask or downplay the impact of an incident. They may feel ok one day but need targeted support the next. Responses may need to be escalated or de-escalated depending on the situation or new information coming to hand.	**Rating**
• Target appears to be coping well. • Target has a supportive peer group and/or family. • Target can manage with minimal support.	0
• Target appears to be coping well with intervention/short term support from adults. • Target requires additional school-based wellbeing support (counsellors/nurses/pastoral care workers/chaplains).	1
• Target has identified vulnerabilities. • Target needs ongoing support from school and/or specialist support.	2
• Target is at immediate or significant risk of harm (call Triple 000). • Target has previously self-harmed or expressed suicidal ideation. • Target is experiencing significant physical, psychological or emotional impact. • There is significant impact on other students and the wider school community.	3

Based on: Netsafe - Bullying Prevention and Response Guide

Reference Guide – Mild incidents

UNDERSTAND AND ASSESS

- *Reassure students that they have done the right thing by reporting the incident.*
- *Consider the best interests of the student/s involved - this should guide a response.*

MANAGE THE RESPONSE

- *Manage the response internally in line with behaviour management wellbeing and online safety policies and procedures.*
- *Focus on providing support for all students and involve them in decision making.*
- *Explain the process and potential outcomes to all involved.*
- *Consider whether involving parents/carers would help to resolve the situation.*

RESOLVE THE CONFLICT

- *If a student/s knows strategies and can respond appropriately, only minimal teacher intervention may be needed beyond supporting students.*
- *Focus on restoring relationships and ensuring all students feel safe and supported.*
- *Address behaviours and provide education about acceptable use and respectful online behaviour.*
- *Encourage students to delete the inappropriate content and/or report it to the social media service.*

RECORD AND REFLECT

- *For younger students, let parents/carers know that there has been an issue. Explain how the issue has been resolved, unless there is a good reason not to involve parents/carers - for example, because it causes further harm.*
- *For older students, their level of maturity and autonomy should be considered, as well as whether it is appropriate to let them tell their parents/carers first.*
- *Record the incident, response and actions taken.*

MONITOR

- *Monitor whether the behaviour has stopped.*
- *Regularly check that students feel safe and supported. Adjust plans if necessary.*

Reference Guide – Moderate incidents

UNDERSTAND AND ASSESS

- *Reassure students that they have done the right thing by reporting the incident.*
- *Consider the best interests of the student/s involved - this should guide a response.*

MANAGE THE RESPONSE

- *Manage the response internally in line with behaviour management wellbeing and online safety policies and procedures.*
- *Focus on providing support for all students and involve them in decision making.*
- *Explain the process and potential outcomes to all involved.*
- *Consider whether involving parents/carers would help to resolve the situation.*

RESOLVE THE CONFLICT

- *Focus on restoring relationships and ensuring all students feel safe and supported.*
- *Address behaviours and provide education about acceptable use and respectful online behaviour.*
- *Encourage students to delete the inappropriate content and/or report it to the social media service.*

RECORD AND REFLECT

- *Let parents/carers know that there has been an issue. Explain how the issue has been resolved, unless there is a good reason not to involve parents/carers - for example, it causes further harm or hampers a police investigation.*
- *Debrief with staff and students, where appropriate.*
- *Record the incident, response and actions taken.*
- *Review exisiting policies and procedures following the incident.*

MONITOR

- *Monitor whether the behaviour has stopped.*
- *Regularly check that students feel safe and supported. Adjust plans if necessary.*

Reference Guide – Serious incidents

CALL TRIPLE 000 IF A STUDENT IS AT RISK OF IMMEDIATE HARM.

UNDERSTAND AND ASSESS

- *Reassure students that they have done the right thing by reporting the incident.*
- *Consider the best interests of the student/s involved - this should guide a response.*
- *Be aware that some cases may be unlawful and may activate state and territory critical incident or mandatory reporting requirements. Always seek support from the school Principal/school leadership team when responding.*

COLLECT AND PRESERVE EVIDENCE

- *Gather facts and document what has happened.*
- *Do not view or copy explicit images.*
- *For non-explicit material, where possible, take screenshots or records URL's.*
- *Check state, territory or school policy. Only confiscate or search students' personal devices with informed consent or if permitted by policy.*

MANAGE THE RESPONSE

- *Focus on providing support for all students and involve them in decision making.*
- *Determine who to inform and when to involve others (eg. parents/carers, other staff or students)*
- *Engage parents/carers as soon as possible so that the school and the family can work together to respond to the incident, unless there is a good reason not to involve parents/carers, for example when it causes further harm or hampers a police investigation.*
- *Explain the process and potential outcomes to all involved.*

REMOVE THE CONTENT

- *If material is circulating and causing harm, and evidence has been collected and preserved, encourage students to delete the material and/or report it to the social media service where it was posted.*
- *If cyberbullying content has not been removed 48 hours after a complaint was made to the social media service, lodge a complaint with eSafety, making sure that the student has given their permission.*
- *For cases of image-based abuse, lodge a complaint with eSafety, making sure the student has given their authorisation.*

RESOLVE THE CONFLICT

- *Focus on restoring relationships and ensuring all students feel safe and supported.*
- *Address behaviours and educate on acceptable use and respectful online behaviour.*
- *Assess whether school-wide communication is appropriate and or what type of intervention is required, such as engaging external providers or support services.*
- *Consider referring students to external organisations such as Kids Helpline for ongoing or one-off counselling if required.*

RECORD AND REFLECT

- *Record the incident, response and actions taken.*
- *Complete a Post Incident Checklist.*
- *Review exisiting policies and procedures following the incident.*
- *Debrief with staff, students and parent/carers where appropriate.*
- *Explain the process and potential outcomes to all involved.*

MONITOR

- *Monitor whether the behaviour has stopped.*
- *Regularly check that students feel safe and supported. Adjust plans if necessary.*

Reference Guide – Severe incidents

CALL TRIPLE 000 IF A STUDENT IS AT RISK OF IMMEDIATE HARM.

UNDERSTAND AND ASSESS

- *Reassure students that they have done the right thing by reporting the incident.*
- *Consider the best interests of the student/s involved - this should guide a response.*
- *Be aware of mandatory reporting obligations.*

SUPPORT STUDENT SAFETY, WELFARE AND WELLBEING

- *If you are concerned about the safety, welfare and wellbeing of a student or suspect unlawful behaviour - report the matter immediately to the Principal or school leadership team.*
- *The Principal/school leadership team may consult with the child protection/student wellbeing officer before contacting local police or child protection agency.*
- *The Principal/school leadership team should contact local police and/or make a report online for cases of online grooming or inappropriate behaviour towards children online, for example:*
  - *adults making online contact with a child under 18 with the intention of facilitating a sexual relationship; or*
  - *an adult accessing, sending or uploading sexualised material depicting someone under 18.*

COLLECT AND PRESERVE EVIDENCE

- *Gather facts and document what has happened.*
- *Do not view or copy explicit images.*
- *For non-explicit material, where possible, take screenshots or records URL's.*
- *Check state, territory or school policy. Only confiscate or search students' personal devices with informed consent or if permitted by policy.*

MANAGE THE RESPONSE

- *Engage parents/carers as soon as possible so that the school and the family can work together to respond to the incident, unless there is a good reason not to involve parents/carers, for example when it causes further harm or hampers a police investigation.*
- *Focus on providing support for all students and, where appropriate, explain the process and potential outcomes to all involved.*
- *Consider referring students to external organisations such as Kids Helpline for ongoing or one-off counselling to all involved.*
- *Focus on providing support for all students and involve them in decision making.*

REMOVE THE CONTENT

- *If material is circulating and causing harm, and evidence has been collected and preserved, encourage students to delete the material and/or report it to the social media service where it was posted.*
- *If cyberbullying content has not been removed 48 hours after a complaint was made to the social media service, lodge a complaint with eSafety, making sure that the student has given their permission.*
- *For cases of image-based abuse, lodge a complaint with eSafety, making sure the student has given their authorisation.*

RECORD AND REFLECT

- *Record the incident in your school incident management system (or via school reporting documents) and follow up according to school or sector policies and procedures.*
- *Complete a Post Incident Checklist.*
- *Review exisiting policies and procedures following the incident.*
- *Debrief with staff, students and parent/carers where appropriate.*

MONITOR

- *Monitor whether the behaviour has stopped.*
- *Regularly check that students feel safe and supported. Adjust plans if necessary.*

Supporting students

Tips for supporting students in an online incident

This resource provides practical tips to support the safety and wellbeing of students involved in an online incident. These tips should assist in planning a comprehensive response that involves the student/s, parents/carers and support services (as appropriate). Support for peers, bystanders and siblings may also need to be considered as part of this process.

Research indicates a notable overlap between students who are the target of negative online behaviour and those who engage in it. This may be a barrier to some students making a report. Regardless of the student's role in the incident, they may feel heightened emotions such as anger, fear or shame. It's important to reassure any student involved and encourage them to report incidents, even when they may have also engaged in negative behaviours or contributed to online conflict/abuse.

Reassure

Remember to remain calm and non-judgemental when talking with a student about an online safety incident. Reassure them that there are steps in process to address the incident and that you will support them through it. Avoid making unrealistic promises. Recognise that for some students it might be difficult to ask for help and let them know that they have done the right thing by coming to you.

Stay calm and listen

It will be easier to learn the specifics of the incident if you remain calm and listen. You might like to ask what you can do to make the conversation more comfortable. Ask open ended questions, for example: 'If you're comfortable talking with me, tell me why we are here today and start at the beginning'. Let those involved know who else they can approach for support and advice through the process. Consider informing them that you may have to tell others what has happened, for example if anyone is at risk of harm (as per mandatory reporting obligations). Drawing on trauma informed approaches may help to provide support during the disclosure process.

Ask students how they would like to resolve the problem

Where appropriate, ask the student/s what steps they would like to see implemented to resolve the problem. While there are procedures to follow when an incident occurs, students have a right to participate in decisions about their life. Being involved in the solution may give them a sense of empowerment in what may feel like a powerless situation.

Communicate with students and parents/carers

If appropriate, work closely with the parents/carers of involved students and their support network (siblings and friends). It is important to maintain clear communications with everyone involved. Lack of clarity about actions and time frames can lead to anxiety, upset and anger. Set a schedule to review actions and make expectations clear to avoid the chance of miscommunication or misinformation.

Part of the process may involve reporting the incident within the school, to the education department, school board or to an outside agency. If required, and it is appropriate to do so, explain to students why these steps are being taken and what will happen next. Let students know you will keep them informed, where appropriate. Schedule check-ups with all students involved to support their wellbeing and ensure that negative behaviours have stopped.

Involve student wellbeing staff

Consider involving other support people through the process, such as a trusted teacher, school counsellor, chaplain or psychologist. You might like to provide the student/s an opportunity to nominate a support person.

Engage with student wellbeing support staff (counsellors/nurses/pastoral care workers/chaplains) to select resources for students to develop help seeking behaviours and build their resilience. Behaviour and learning support for the student who instigated the online incident should also be considered.

Your student wellbeing support staff should be able to assist in selecting an appropriate social and emotional learning, respectful relationships or conflict management approach.

Support for bystanders, peers, siblings

Staff should be aware of the impact of online incidents on students involved, including bystanders, and provide support for these students. Students may discuss their experiences with friends, siblings or in the classroom. This is a normal response to a difficult incident. Staff can help to keep the tone of conversations positive, and the focus on help seeking. Normalising conversations around online safety will help to remove stigma around reporting and support students to develop help-seeking behaviours.

Counseling and support services

The eSafety website includes a list of counselling and support services that can help anyone involved in an online safety incident. This list can be filtered by audience, the type of support required, issue and state/territory. Your education department or sector may also offer tailored support services.

Resources

- headspace — support following large scale incidents
- National Office for Child Safety Complaint Handling Guide
- Blue Knot Foundation — fact sheets for talking about trauma
- Bullying. No Way! — How Australian schools respond

Post Incident Checklist

Post Incident checklist	Yes
Immediate response	
1. Did the students involved in the incident know who to ask for advice and/or know how to report the incident? • Establish specific roles and responsibilities among staff (e.g. an online safety team) so that all members of the school community know who they can report to. Even if a student reports to their classroom teacher, an online safety team can provide additional advice and assistance to resolve the incident. • Make incident response procedures publicly available. Schools can display these high-traffic areas and on their website. • Schools can invite suggestions from students about how to make the reporting process easier and should consider having multiple reporting pathways available, such as an anonymous online reporting mechanism or access to student wellbeing support staff.	□
2. Did the staff member/s responding to the incident try to understand the context to accurately assess its severity and impact? • Schools are encouraged to provide training for all staff in responding to incidents. eSafety's Responding to online safety incidents - Teacher professional learning presentation can support good practice. • The circumstances of any particular incident can make it difficult to know how to respond. • eSafety's Online incident assessment tool also supports good practice.	□
Support wellbeing	
3. Was support provided to all students involved in the incident (e.g. the target, instigator or bystanders)? • Offer support to students throughout the incident response process and help them to seek support if they need it. Provide support for peers, bystanders and siblings as part of this process. • Engage with student wellbeing support staff (e.g. counsellors, nurses, pastoral care workers, chaplains) as early as possible to develop an appropriate support plan. • eSafety's Tips for supporting students involved in an online incident resource can help to support good practice.	□
4. Have wellbeing checks been scheduled with all students involved in the incident (i.e. target, instigator and bystanders)? • Schedule follow-ups as part of any response and assign actions to relevant teachers or wellbeing staff. Involve parents/carers in the process and keep them up to date, where appropriate. • Consider whether the students involved are likely to need or want ongoing support. This might include support that you can provide internally, or with external support services. • Adjust your response if, during a wellbeing check, you identify that a student requires additional support or is experiencing unintended negative consequences from the incident. • Check the eSafety website's list of counselling and support services to help those involved in an online safety incident. This list can be filtered by audience, the type of support required, issue and state/territory.	□

Post Incident checklist	Yes
Support wellbeing (continued)	
5. Were all parties involved in the incident — target, instigator, bystanders, parents/carers and staff — debriefed and made aware of the resolution? • Debriefing with students, parents/carers and staff shortly after an incident can provide clarity on the steps taken to resolve an issue and aid resolution. • Parents/carers who are concerned for their children can feel frustrated by a lack of communication from schools following an incident. Debriefing provides an opportunity to make them aware of any issues and have their voices heard during the resolution process. • Debriefing can support students to regain a sense of safety and wellbeing, allowing them to re-engage with the school. • If the incident occurred outside school hours, but was managed by the school, schools should work in partnership with parents/carers to resolve the issue. eSafety's Tips for responding to incidents that happen outside school hours and Tips for parents/carers after an online safety incident resources can support good practice. • Remind staff that they have access to employee assistance programs, wellbeing representatives and external agencies that can provide additional support when responding to online safety issues.	□
External involvement	
6. If the incident involved harmful content circulating online, was the content removed? • A clear first step is to contact the social media site to request the content to be removed. The eSafety Guide has links to the latest games, apps and social media, with tips on how to contact a platform or website directly to request content be removed. • Remember that the eSafety Commissioner can help to take down serious cyberbullying material, image- based abuse material or prohibited online content. • If the incident requires police involvement, schools should seek police guidance about removing content, as it may be considered evidence.	□
7. If there was media coverage of the incident, was the situation handled in a way that supported student safety and wellbeing? • Media involvement in a school incident can be stressful for all parties involved. Having clear processes about how to manage this can help to alleviate stress and support student safety and wellbeing. • Depending on your education sector, there may be specific procedures for how schools engage with the media. Schools should contact the relevant media unit/team in their education department/sector or school board for guidance. eSafety's Guide to engaging with the media resource can help.	□
8. If police, child protection or other external agencies were involved, have the students, parents/carers and teachers involved in the incident been appropriately debriefed? • External engagement in a school incident can be stressful, particularly if the external agency is managing the incident. Debriefing, where appropriate, and closing the loop with external agencies can help to alleviate this stress and supports the safety and wellbeing of students. Note: Depending on the nature of the incident, police may exclude the school from further updates about the matter. However, police may offer external support to students, parents/carers and staff through targeted sessions.	□

Post Incident checklist	Yes
Finalising the response	
9. Was a record of the incident collected and stored in a safe and secure location? • Incidents Should be recorded in your school incident management system (or via school reporting documents). Information should be captured, and records kept, in line with education department, sector or school policies. When recording incidents remember that: – incidents should be stored securely with password or restricted access and be consistent with relevant privacy legislation. – detailed records can contribute to a robust and defensible approach to online incidents. – incident records may be used if police or legal involvement is required. In these circumstances, schools, students or their parents/carers may need to seek legal advice. – collecting and reviewing incident data and feedback can help to identify trends, wider issues and behaviour patterns in a school. This data can be used to improve procedures and responses.	□
10. Has the inappropriate behaviour stopped? • If an issue is recurring or is becoming widespread, more comprehensive and targeted online safety education could help. The eSafety website offers a range of classroom resources, which can be filtered by year level and topic. • Engaging parents/carers to help reinforce positive behaviours at home and guide their children to have safer online experiences may be useful if the issue has not been resolved appropriately. eSafety's Tips for parents/carers after an online safety incident can support good practice. • Seeking external agencies to partner with the school can also assist with ongoing issues. The eSafety website includes a list of counselling and support services that can help those involved in an online safety incident. This list can be filtered by audience, issue, type of support required and location.	□
11. Are procedural or policy changes required to prevent this issue from recurring? • Record your 'lessons learned' and use them to inform updates to school policies and procedures. Use this data to brief the school leadership, wellbeing or online safety teams, as appropriate, to support continuous improvement in responses. • Encourage staff to undertake professional learning about how to respond to incidents. eSafety's Responding to online safety incidents - Teacher professional learning presentation can support staff to practice their skills. • eSafety's Online safety self-assessment tool and Checklist for developing effective school policies and procedures can support good practice.	□