



10 Lacey's Rd, PO Box 140, Cottles Bridge VIC 3099 Phone: 9718 1481
info@learningcooperative.vic.edu.au www.hurstbridgelearningcoop.vic.edu.au

Learning Co-operative e-Safety Policy

Rationale/Introduction

1.1 The Learning Co-operative is committed to using technology as an important resource to support teaching and learning. We will develop and implement online safety policies and procedures, tailored to the needs of our learning community.

1.2 All children will have access to computers and sometimes tablets and digital cameras for web-based and mobile learning at the Learning Co-operative. Currently the internet technologies children are using either during or outside of school include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Blogs
- Video Broadcasting and Instant Messaging
- Email
- Podcasting
- Music downloading
- Gaming
- Mobile/Smart phones with text video and/or web functionality
- Other mobile devices with web functionality

1.3 The Learning Co-operative is committed to focusing on a model of guided empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly and managing risks.

1.4 The Learning Co-operative has a duty of care to provide a safe environment for all children, including a safe online environment, in accordance with the Child Safety and

Wellbeing Policy, the Child Safe Standards and the National Principles for Child Safe Organisations.

- 1.5 The Learning Co-operative also uses technology for communication between parents and staff, maintaining a website and a social media presence and for organising and storing data and has a duty of care to all employees and members of the school community to provide a safe online environment and respect privacy in line with the Record Management and Archiving Policy, Privacy Policy and the Privacy Act 1998.
- 1.6 The e-Safety Policy reflects the need to raise awareness of the safety issues associated with information systems, data and electronic communication for the school community.
- 1.7 All members of the school have a responsibility for promoting and supporting safe online behaviour both at home and at school.

2. Aims

Through the application of this policy, we at the Learning Co-operative aim to employ a whole school approach to e-safety by:

- 2.1 Including e-safety in the school curriculum
- 2.2 Managing internet usage for children appropriately
- 2.3 Ensuring safe use of email, social media and school communication channels.
- 2.4 Ensuring safe use of digital images and digital technologies such as mobile phones and digital cameras and permitted publication of pupil information/photographs on the school website
- 2.5 Ensuring safe use of Learning Platforms and Virtual Learning Environments
- 2.6 Ensuring staff and the community are aware of safe use of online data and data protection.
- 2.7 Ensuring staff, students and the community are aware of the e-Safety Policy and the staff and kids technology agreement.
- 2.8 Ensuring staff and parents are trained and informed in e-safety.
- 2.9 Raise awareness of cyberbullying, and strategies for minimising the risk of cyberbullying.

- 2.10 Outline steps for responding to and investigating online incidents that are consistent with the processes and protocols outlined by the Commonwealth Commissioner of eSafety.
- 2.11 Outline procedures for complaints in the event of misuse of technology by any member of the school community

1. Roles and Responsibilities

All members of the school community have a responsibility for promoting and supporting safe behaviour in school and at home and following school e-safety procedures.

The Principal, Child Safety Team and the parent volunteer IT Support Team will ensure they are up to date with current guidance and issues through organisations such as ISV (Independent Schools Victoria), DET (Department of Education and Training), e-Smart and the eSafety Commissioner and update other teachers and parents as necessary.

2. Scope

All staff, CRTs, school governors and parents should be familiar with the e-Safety Policy:

- safe use of e-mail
- safe use of the Internet
- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on the school website
- procedures in the event of misuse of technology by any member of the school community
- their role in providing e-safety education for pupils.

3. Students with additional needs and requirements

4.1 We will address equal opportunity and anti-discrimination practices as part of the school's duty of care to provide respectful, safe and inclusive school environment which is, free of discrimination, harassment, bullying, vilification, victimisation and otherwise unlawful and unacceptable behaviours. Equal opportunity and anti-discrimination are covered in a range of commonwealth and state laws.

4.2 We will offer training and supervision to our school community to proactively identify and consider the needs of vulnerable students who may be more at risk of either engaging in bullying behaviour or being the victim of bullying behaviours. At risk students may include those with special educational needs and/or with a disability, racial and minority groups and those who are potentially the subject of homophobic bullying.

4. Supporting Documents

Kids Safe Use of Technology Agreement (appendix 1)

Staff/Governor/Volunteer Safe Use of Technology Agreement (appendix 2)

Risk Assessment Template for New Technology (appendix 3)

Common types of Cyberbullying (appendix 4)

Cyberbullying Information Sheet for Parents (appendix 5)

e-Safety Incident Assessment Tool (appendix 6)

e-Safety Incident Response Flow Chart (appendix 7)

e-Safety Post incident evaluation checklist (appendix 8)

5. Implementation

All staff, parent teacher volunteers, CRTs and students must sign a Safe Use of Technology Agreement (see appendix 1 and 2).

6.1 e-Safety in the curriculum

Technology and online resources are increasingly used across the curriculum. The Learning Co-operative believe it is essential for e-safety guidance to be given to the pupils on a

regular basis. We continually look for new opportunities to promote e-safety. Resources from the [e-Safety Commissioner](#) are employed, and the school is registered with eSmart.

- We will provide opportunities within the Digital Technology, Health and Physical Education curriculum and Personal and Social capability to teach about e-safety.
- Educating pupils on the dangers of technologies that may be encountered outside school will be done informally when opportunities arise, as part of the curriculum and through communication to parents/caregivers.
- Pupils will be taught about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities as part of the Digital Technology curriculum and when they are using technology in other curriculum areas.
- Pupils will be made aware of the impact of online bullying through Health and Well Being sessions and will be taught how to seek help if they are affected by these issues. Pupils will also be made aware of where to seek advice or help if they experience problems when using the internet and related technologies (cyber bullying)
- Pupils will be taught to critically evaluate materials and learn safe searching skills through cross curricular teacher models, discussions and via the Digital Technology curriculum
- Pupils will be taught about the risks inherent in using social media, particularly if they are contacted by people they do not know.
- The school will explore taking part in annual whole school events, such as the annual National eSmart Week from the Alannah & Madeline Foundation and Cybersafety days.
- Students are familiar with the notion of 'consent' (i.e. asking for and giving permission) with regard to the taking of and publication of digital images.

6.2 Managing Internet Access

Children will only have supervised access to Internet resources and cannot access the Internet if unsupervised by an adult at school or on school excursions/camps.

- Staff must preview any recommended websites before use. Particular care must be taken when using search engines with the children as these can return undesirable links.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework or remote learning, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents need to be advised to supervise any further research.
- Students are encouraged to use Google 'safe search kids' and 'kidztube' to filter internet content. Parents will be encouraged to use internet filters at home. We will explore other internet filters on school computers.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Principal or Child Safety Officer.
- It is the responsibility of the school, by delegation to the School Admin team, to ensure that antivirus protection is installed and kept up-to-date on all school machines.
- Students are encouraged to set timers so that they are only using digital technology for a maximum of 30 minutes in one sitting before taking a break.
- A computer logbook is used to ensure fair use of computers by different students.

6.3 E-mail, Website, and Social Media Channels

Email, Whats App and Slack are used within school as an essential means of communication for staff and parents. The school has an active social media channel on Facebook. Students do not have school email addresses but some older children (Year 6) have their own home email address. The school uses admin computers, back-up drives and the google drive to store data in accordance with the Record Management and Archiving Policy and the Privacy Policy.

- The school gives staff their own school email account, to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Staff should not contact pupils or parents using personal email addresses.
- In the context of school, email should not be considered private.
- Pupils may only use email at school under direct teacher supervision for educational purposes.
- Some pupils have emails at home and will be told to immediately tell a trusted adult/teacher if they receive an offensive e-mail. Parents will be encouraged to teach them how to block unknown email addresses on their home email accounts.
- All pupils must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Staff or members of the community must follow the Complaints and Grievances Policy if they receive an offensive e-mail from others in the community.
- Whats App and Slack is for staff and parent communication only. Language must be respectful and debates should not be started through these forums, they should be addressed in face-to- face meetings.
- The Principal, Child Safety Officer and Admin Officer have access to school social media on Facebook and the school website.
- The website and social media channel are set up for school communications not complaints.
- The school media accounts have secure login, and authentication procedures and are monitored regularly. Inappropriate posts are removed.
- Acceptable use of the school's name and logo online will follow the ?communication policy
- Social media may be used by staff to support student learning if there is an appropriate educational purpose.
- Social media use must be planned, be reflected in school-based curriculum documents, and be approved by the school principal or their nominee(s).
- Staff use of social media to support student learning must be consistent with the professional conduct, personal conduct and professional competence expected of a teacher by their colleagues and the community.

- Social media use must in all cases comply with relevant legislation and Department policies, including in relation to staff conduct, privacy, copyright, information security and child safety.
- Any social media student activity visible to the public must not proceed without consent.

6.4 Pupil's images

On a child's entry to the school, all parents/guardians will be asked to give permission for their child's photo to be taken and to use their child's work/photos in the following ways:

- on the school web site
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)

Pupils' names will not be published alongside their image and vice versa without permission from the parents.

Full names will not be published.

Pictures will not be published if it places a student at risk of harm, for example, where there are legal proceedings or a court order relating to child protection, custody, domestic violence or family separation.

We recognise that a student's cultural background may be a determining factor in how their images can and cannot be used.

Children's photos must be taken on the school digital cameras and must never be stored on personal devices.

6.5 Learning Platforms and Virtual Learning Environments

Virtual Learning Platforms such as [Zoom](#), Reading Eggs, Nessy, SCRATCH and [Seesaw](#) are an important tool for learning, particularly remote learning.

- New technologies will be risk assessed before being adopted (see appendix 3)
- Communication will be made with parents when online accounts are created for students and to share the strategies being used to keep students' identities safe.
- Parents and students will be told of the importance of keeping passwords for Virtual Learning Platforms private.
- Students will be taught to use usernames that don't identify their name, age or gender.
- For Zoom, parents are asked to be in the room when their child is using zoom. Particularly during individual sessions. Meetings are scheduled with new links and passcodes each time, and never posted publicly, for example, on the website/social media, to avoid the risk of people outside the community accessing links. Students are not able to join before the host and waiting room is enabled to prevent unknown people from joining the meeting. Children are encouraged to have their cameras turned on. Photo virtual backgrounds of people will be discouraged. Zoom guidelines are emailed to parents and available on the virtual learning website.

6.6 Safe use of data

Personal data will be recorded, processed, stored, transferred and made available according to the school Privacy Policy, based on the Privacy Act 1998 and the procedures outlined in the Record Managing and Archiving Policy.

Sensitive data or photos and videos of students will be stored securely with restricted or password protected access.

6.7 Communication of e-Safety

e-Safety is an integral part of the Learning Co-operatives commitment to providing a safe environment for all members of the community. Staff and the school community are reminded/updated about e-safety regularly at student and adult meetings and through the curriculum (as outlined above 5.1).

Resources from the e-Safety Commissioner will be used to engage parents in topics around e-safety. Parent training webinars will be booked through eSmart and the eSafety Commissioner and details communicated to the group.

Posters on e-safety are displayed near to the computers to remind staff, parents and students of safe use of technology and how to report incidents.

All students should be familiar with the Kids Safe Use of Technology Agreement (see appendix 1).

Inductions ensure new staff, students and the community are aware of the e-safety policy and the staff and kids technology agreement.

Casual Relief Teachers must sign a Staff Safe use of Technology Agreement before using technology equipment in school (see appendix 2).

New staff, parents and students receive information on the school's Safe Use of Technology Agreement as part of their induction/ enrolment pack.

6.8 e-Safety Training

e-Safety is part of the training schedule developed through the Child Safety and Well Being Policy. The Learning Co-operative is committed to providing training to staff, Board members and members of the parent community on an annual basis as this area is one of rapid development and change.

The Principal, Child Safety Officer and the Board will be responsible for keeping training up to date in areas impacting on e-safety.

Parent training and webinar opportunities will be advertised in the community.

6.9 Cyberbullying

Cyberbullying is the use of technology, particularly mobile phones and the internet, to deliberately upset someone else. The Learning Co-operative has a strong 'no bullying' attitude and promotes respectful relationships through the school Anti-bullying Policy and Child Safety and Well Being Policy. The whole school community has a duty to protect all its members and provide a safe, healthy environment.

Although bullying is not a specific criminal offence, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications.

There are many types of cyberbullying, these are listed in appendix 4.

Preventing Cyberbullying

It is important that we work in partnership with pupils and parents to educate them about cyberbullying as part of our e-Safety curriculum.

They should:

- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are being cyber bullied.
- report any problems with cyberbullying. If they do have a problem, they can talk to a trusted adult, the Child Safety Officer, the Principal, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.
- Make a complaint through eSafety Commissioner [Cyberbullying | eSafety Commissioner](#))
- [Report abuse | eSafety Commissioner](#)

- Contact Kids Helpline for support at <https://kidshelpline.com.au> or phone (1800 55 1800) or 13 22 89
- Contact eHeadspace for young people 12 years plus for support at <https://headspace.org.au> or phone (1800 650 890)

See appendix 5 for Key Safety Advice for children, parents and carers

Supporting the Person Being Bullied

Support shall be given in line with the Antibullying Policy.

- Give reassurance that the person has done the right thing by telling someone and inform parents.
- Make sure the person knows not to retaliate or return the message.
- Help the person keep relevant evidence for any investigation (taking screen capture shots if appropriate, not deleting messages.)
- Check the person knows how to prevent it from happening again e.g. blocking contacts, changing contact details.
- Take action to contain the incident when content has been circulated: remove content, contact the host (social networking site) to get the content taken down, use disciplinary powers to confiscate phones that are being used to cyber bully – ask the pupil who they have sent messages to.

Further support for parents is available at:

- [eSafety Commissioner Advice for Parents](#)
- [Parentline VIC](#)
- [Help — Counselling and Support Online](#) (eSafety Commissioner website)

Investigating Incidents

All cyberbullying incidents should be recorded in the incident log as any other bullying incident. We will then investigate fully as any other bullying incident.

Incidents Out of School Hours:

The Learning Co-operative has a duty of care to respond to online incidents that happen outside of school hours. If the incident is affecting the well being of the student, staff will take steps to support and provide strategies to assist them. We will work in partnership with students, parents and support services where required, considering the rights, views and wishes of the child involved.

6.10 Reporting and responding to e-safety incidents

The school will encourage a positive school climate and a culture of help-seeking that supports students to feel safe and comfortable to report online incidents to a trusted adult, Child Safety Officer or the Principal.

Any accidental access of inappropriate material must also be reported immediately to the e-Safety Officer, Child Safety Officer or the Principal.

If an incident is reported an incident assessment tool from the e-Safety Commissioner (appendix 6) will be used to determine whether the incident is classed as severe, serious, moderate or mild.

The level of the incident will determine the response employed (appendix 7).

6.11 Responding to e-safety complaints

As a school we will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access.

Complaints relating to e-safety, or staff misuse should be made to the Principal or the Board in line with the Complaints and Grievances Policy. All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence; investigation by the Principal and Board and involvement of police for very serious offences as per the Child Safety Policy.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

Evaluation

There will be an on-going opportunity for staff and parent to discuss with the Principal any issue of e-safety that concerns them.

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed (Appendix 3). The Learning Co-operative will endeavour to use software, online products and collaboration tool with the highest safety, privacy, and security standards possible.

The policy will be amended if new technologies are adopted or with new guidance from ISV or DET.

The success of the schools' response to an online incident will be evaluated with a post-incident checklist (appendix 8) to ensure we have met our duty of care and to inform future responses.

This Policy was ratified by the board of The Learning Co-operative **11/10/2021**

This policy will be reviewed every year or with the implementation of new technology.


Chairperson's signature



.....
(MYRA THEISZ)

Version and revision control record

Previous policy known as Internet Usage Policy – can be found in archive

Date	Version	Approver	Next Review Date
15/10/2021	2	Name: MYRA THEISZ Position: Chairperson of the School Board Signature: 	October 2022

Appendix 1 Safe Use of Technology Agreement Kids

Dear Parent/ Carer,

The use of technology including the Internet, learning platforms and today's mobile technologies are an integral element of learning in our school. In making this as successful and as beneficial as possible for all learners, we expect all pupils to act safely and responsibly when using technology both within, and outside of, the school environment. We review our e-Safety Policy annually and have just updated our Safe Use Agreement.

The enclosed Safe Use of Technology Agreement forms part of the wider School e-Safety Policy and in association with the school's Behaviour Management Policy, outlines those principles we expect our students to uphold for the benefit of both themselves and the wider school community. I would therefore ask that you please read and discuss the enclosed Safe Use Agreement with your child and return the completed slip at the bottom of this page as soon as possible.

if you would like to find out more about eSafety for parents and carers, please visit the eSafety Commissioner website at <https://www.esafety.gov.au/>. There is a range of parental control software available online (either free or for purchase) which you may like to consider if you have not got this already.

If you have any concerns or would like to discuss any aspect of eSafety, please contact the school office for further guidance.

Kind regards

Liz Bennet

Safe Use of Technology Agreement for students:

- I will take care when using the school computers, tablets and digital cameras and use them properly
- I will only share my user name and password with trusted adults
- I will tell an adult if I see anything that upsets me
- I will use a safe name and not my real name on the internet
- I know I am only allowed to go on the internet if my teacher has given me permission
- I will only take a photograph or video of someone if they say it is alright
- Any messages I send will be respectful
- I will not deliberately write anything which upsets other people
- I understand that the school may talk to my parent or carer if they are worried about my use of school IT equipment
- I understand that if I do not follow these rules I may not be allowed to use the school computer or internet for a while, even if it was done outside school

Parent/ Carer signature

We have discussed this and (childs name)

agrees to follow the eSafety rules and to support the safe use of technology at the Learning Cooperative

Parent / Carer Name (PRINT)

Parent / Carer (Signature)

Date.....

Appendix 2 Safe Use of Technology Agreement

Staff, Governor, Volunteer and Visitor

Safe Use of Technology Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff and volunteers are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the Co-ordinator.

- I will only use the school's email / Internet / Learning Platforms and any related technologies for professional purposes or for uses deemed 'reasonable' by the Co-ordinator or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. USB sticks containing data must be encrypted.
- I will not use or install any hardware or software without permission from the Child Safety Officer.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken with school devices, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school

network without the permission of the parent/ carer, member of staff or headteacher.

- I understand I cannot use my mobile phone to take photos of children
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Co-ordinator or the Board.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature Date


Full Name (printed)


Job title:













Appendix 3: Risk Assessment Template for New Technology (Source: e-Safety Commissioner accessed Sep 21)

Important note
















This risk-assessment tool is not exhaustive and should be adapted to individual school circumstances. It does not replace legal advice regarding statutory and common law obligations to assess risks. The decision to use certain technologies or platforms should be made in line with a school's risk management procedures and child safety policies. School leadership teams may wish to take appropriate legal advice when making these decisions.

 Risk identified: take appropriate action to mitigate risks before using

 Proceed with caution: continue to monitor for risks

Consider	Yes	No	Suggestions to mitigate risks
Will students' personal information be publicly displayed (e.g. photograph, date of birth, gender or name of school)?			<ul style="list-style-type: none"> Obtain consent from students and their parents/carers before displaying personal information online. Where possible, de-identify student information.
Can external, unauthorised users communicate with students?			<ul style="list-style-type: none"> Install appropriate technologies to monitor and filter activities on school ICT systems. Teach students strategies to report external, unauthorised communication and block inappropriate content or contact.
Does the platform encourage students to use their existing email or social networking accounts for sign in or use?			<ul style="list-style-type: none"> Often platforms also have the option to sign up or log in using unique usernames and passwords. While using existing social networking accounts might be quicker, unique logins are a safer option. Teach students the importance of strong passwords and not sharing passwords.
Are student profiles linked to apps that can display their location?			<ul style="list-style-type: none"> Teach students strategies to turn off location services functions, or to block apps that have these turned on.
Does the education department prohibit the use of this technology or platform?			<ul style="list-style-type: none"> If the education department's policies prohibit the use of this technology or platform it is recommended not to use it.
Can students access inappropriate content using this technology or platform?			<ul style="list-style-type: none"> Install appropriate technologies to monitor and filter activities on school ICT systems. Encourage help-seeking behaviours so students know the steps to take if they come across inappropriate content.

1

Consider	Yes	No	Suggestions to mitigate risks
Have minimum age requirements for the technology or platform been adhered to?			<ul style="list-style-type: none"> Check age appropriateness prior to use. Teach students about age recommendations and the reasons behind them.
Does the platform promote privacy and security for students and their accounts?			<ul style="list-style-type: none"> Empower students to protect their privacy and explain how to adjust security settings.
Have parents/carers consented to their child using this technology or platform?			<ul style="list-style-type: none"> Ensure appropriate consent has been provided by parents/carers. Some schools request consent to use a broad range of platforms at the start of the school year to avoid having to ask for consent each time a new platform is used. It's important to be as clear as possible about what this consent includes, as well as providing information on any possible risks to users and how the school mitigates them.
Are staff comfortable and confident using the platform?			<ul style="list-style-type: none"> Provide access to professional learning so staff are skilled in the platforms/technologies they use.
Is there a staff member moderator for chat or comment functions?			<ul style="list-style-type: none"> A staff member (or team) would ideally be appointed to moderate chat or comment functions, to encourage safe and positive interactions and to take down and investigate inappropriate posts.
Does the platform have capacity to report problems or misuse?			<ul style="list-style-type: none"> All platforms should have terms of use that clearly identify inappropriate content or behaviour, and how to report problems or misuse. Visit The eSafety Guide for more information.
Do all users know how to set the platforms' privacy settings?			<ul style="list-style-type: none"> Share The eSafety Guide with staff. This has links to the latest games, apps and social media, with tips on how to set privacy settings.
Have you identified how data is stored and used by the platform?			<ul style="list-style-type: none"> Privacy issues arise when data is collected and not stored securely or shared inappropriately. Good practice is to find out how data will be stored and who has access. Check education department or sector policies to see if there are any standard protocols schools should follow, as well as advice about privacy legislation and data storage.

Appendix 4 – Common types of cyberbullying

1. Text messages — that are threatening or cause discomfort – also included here is “bluejacking” (the sending of anonymous text messages over short distances using “Bluetooth” wireless technology).
2. Picture/video-clips via mobile phone cameras – images sent to others to make the victim feel threatened or embarrassed.
3. Mobile phone calls — silent calls or abusive messages; or stealing the victim’s phone and using it to harass others, to make them believe the victim is responsible.
4. Emails — threatening or bullying emails, often sent using a pseudonym or somebody else’s name.
5. Chatroom bullying — menacing or upsetting responses to children or young people when they are in web-based chatrooms.
6. Instant messaging (IM) — unpleasant messages sent while children conduct real-time conversations online using MSM (Microsoft Messenger) or Yahoo Chat.
7. Bullying via websites and social networking sites — use of defamatory blogs, personal websites and online personal “own web space” sites.

The best way to deal with Cyberbullying is to prevent it happening in the first place and to have clear steps to take when responding to it.

Appendix 5 Cyberbullying Information for Parents

Source: Bully Stoppers, DET, accessed Sep 21

<https://www.education.vic.gov.au/about/programs/bullystoppers/Pages/advice-sheet-cyber.aspx>

Cyberbullying can be pervasive and incessant. Parents should be aware of what they can do to help.

What is 'cyberbullying'?

Cyberbullying is when someone is repeatedly mean, nasty, horrible, harassing and/or threatening towards another person using any form of digital technology, including social media, mobile phones or online games.

Like any bullying, cyberbullying often occurs between people that know each other—students at the same school, members of a sporting club, people from the same social circle, 'friends of a friend'. If someone is being cyberbullied, they are also likely to be bullied in person.

Cyberbullying is pervasive and incessant. It differs from face-to-face bullying in that the bully can 'follow' their victim home and into their house. This means that it can continue 24/7. Cyberbullies may take advantage of the perception of anonymity (e.g. using an account in a fake name, or a blocked number) but in many cases it is clear who is behind the bullying.

Cyberbullying can be particularly harmful as it is often very public. Usually, many people can see what is written or posted. Once something is published online, it is difficult if not impossible to remove all traces of it. This means the bullying can be ongoing.

Forms of cyberbullying

- sending nasty texts, posts, instant messages, pictures and/or emails. It can also be a humiliating video.
- repeated prank phone calls.
- setting up a fake account in someone else's name and using that to bully and harass.
- using a person's password to access their account and then pretending to be them
- forwarding others' private emails, messages, pictures or videos without permission.
- posting mean or nasty comments online.
- sending and/or forwarding sexually explicit images (see the Sexting advice sheet for more information).
- intentionally excluding others from an online group or chat.

Signs your child may be being cyberbullied

Psychological harm is often harder for parents to identify than the signs of face-to-face bullying, which may include physical injuries. There is no definitive list of signs that indicate cyberbullying but there are some things to look out for:

- change in mood, demeanour and/or behaviour: for example being upset, angry, teary or rebellious when not previously
- change in friendship groups: it can be normal to change friends during the school year but sudden changes should be explored.
- spending more time with family instead of friends: adolescence is generally a time where friends become very important and parents less so. Look out for a child who suddenly wants to be at home all the time.
- lowering of marks: often students who are being bullied show a distinct change in application to studies and a lowering of marks.
- not wanting to go to places: a dramatic change in enthusiasm for going to school or sport— this can manifest as non-specific illness (headaches, stomach-aches, generally ‘feeling sick.’)
- distinct change in online behaviours: being ‘jumpy’ when text messages arrive, not leaving their phone alone, wanting to be online all the time, or never wanting to be online.

Aren't these things normal?

Many of these behaviours may have different causes or may be stages of your child's development. In general, it is important to become the world's best expert on your own child, keep an eye on their behaviour patterns and if you feel something is amiss, explore and let them know that nothing is so bad they cannot tell you about it. Talk early and talk often. Ask them:

If you are still concerned then enlist the help of your school wellbeing staff, GP, a counsellor or psychologist.

What can I do if my child is cyberbullied?

Praise them for coming to you

This is a big step as many young people may be frightened to tell a parent about cyberbullying. Even if you don't really understand, let them know that you will help them.

Do not be angry with your child

Remember that it is someone else who is doing the wrong thing. Do not threaten to take technology away from them because of what someone else has done.

Do not respond to the bullying

It is important not to respond to the abuse. This is usually what the bully wants, so ignore them. It is natural in many cases to want to 'fight back' but responding with abuse or a threat may get your child into trouble as well.

Inform your child's school

It is important that the school knows what is going on so they can provide support and monitor any issues that may spill onto the playground or classroom. If the bully is a student from the same school, the school will work through the situation as they would with any other bullying behaviours reported to them.

Save and store the content

Keep copies of all the abusive communications. Take a screen shot or print out for evidence—ask your child for help to do this if necessary.

Help your child to block and delete the bully from all contact lists

Most social networking sites allow the user to control who has the ability to communicate with them. Many people feel 'mean' blocking another person, even if that person has already been mean to them—you may want to sit and support your child as they do this.

Use the 'report abuse' button

Most social networking sites have a method to let the site administrators know that a particular user is behaving unacceptably. Never hesitate to report abuse to the site—they must act.

Have some 'down time' without technology

It is important for both mental and physical health that your child's life is balanced—so they are not constantly 'online' or spending hours on a mobile phone. This should not be used as punishment, rather as some peaceful time where they are not being bothered.

Use parental controls and restrictions to help manage

Use the parental controls and restrictions on the device to limit or prevent contact, for example, blocking a phone number. Third party apps can also be used. If you need to change a number due to abuse, contact your phone company.

The office of eSafety Commissioner

Serious cyberbullying involving an Australian citizen under the age of 18 years can be reported to the eSafety Commissioner. To learn more, visit www.esafety.gov.au.

If ongoing, report to police

Most cyberbullying between students is usually resolved at school level so ensure that the school is aware and investigating as per their Bullying and/or Student Engagement Policy. This is the first step.

If this is not successful in resolving the situation then you could consider making a report to local police.

There are three main reasons a police report may be necessary:

1. Despite the best efforts of the school, parents or any other responsible adults, the bullying does not stop
2. When it is not possible to know who is behind the bullying (e.g. fake accounts/blocked numbers); or
3. When threats have been made to your child's personal safety.

Cyberbullying is a criminal offence in Victoria as well as every other State and Territory of Australia. There are both State and Commonwealth Laws applicable to this behaviour and you do not have to put up with any form of online bullying.

What if my child is the bully?

It often comes as a shock to be told that your child has been bullying another student online. It is important that parents support schools in their handling of the situation. Don't try and play it down.

Schools have policies and programs to deal with all parties (bully, target and witness), involved in bullying incidents.

Parents can help to prevent online bullying. Be involved, and aware of what your child is doing online. Once you are aware that your child has bullied someone else online, you can help them understand that their behaviour is both unacceptable and possibly criminal as well.

Steps to take

As a parent you could:

- discuss why it is not acceptable to be nasty or mean online and offline
- let them see there are consequences for poor behaviour both on and offline—don't bail them out
- acknowledge that they may be feeling guilty or awful about their behaviour, and discuss ways they can rectify the situation
- work together to improve the situation by offering an apology to the victim and removing posts etc.
- talk to them about their actions and try and find out why they behaved in this way and take steps to ensure it does not continue
- ask them to imagine they were the victim— how would they feel? (try to encourage your child to have empathy for the target)

- if the bullying is on an age restricted social media platform and they are under the specified minimum age of use, they should not have an account. Shut their account down immediately.
- develop a home-based Acceptable Use Agreement—set clear rules and boundaries about their online behaviour and your expectations and consequences for breaching this agreement.
- if the poor behaviour continues or your child cannot see the harms they are causing, enlist the help of your school wellbeing staff, GP, a counsellor or adolescent psychologist. to support both your child and yourself.

The Following documents are also relevant and embedded within the document, Please see the following:

Appendix 6: Incident Assessment Tool- Source e-Safety Commissioner Tool Kit accessed Sep 21

Appendix 7 Response – Source e-Safety Commissioner accessed Sep 21

Response flow chart to mild incidents

Response flow chart to moderate incidents

Appendix 8 Post incident evaluation checklist source e-Safety Commissioner Toolkit accessed Sep 21

Online incident assessment tool

eSafety Toolkit for Schools

Creating safer online environments



This online incident assessment tool provides school staff with a way to assess and determine appropriate responses to a range of online safety incidents. It offers a straightforward starting point and can help staff to plan their approach quickly and effectively and is supported by eSafety's [Guide for responding to serious online safety incidents](#).

Schools should note that the online incident assessment tool is a supporting resource and does not replace decisions based on the experiences of schools, or state/territory or sector policies and processes.

This resource can be used to build teacher capacity as part of teacher professional learning. eSafety's [Responding to online safety incidents presentation](#) offers additional support.

We would like to thank [Kids Helpline](#) for their advice and contributions to this resource.

Disclaimer: This material is general in nature. It is made available on the understanding that the Commonwealth is not engaged in rendering professional advice. Before relying on the material in any matter, you should carefully evaluate its accuracy, currency, completeness and relevance for your purposes and should obtain any appropriate professional advice relevant to your particular circumstances. The Commonwealth does not guarantee, and accepts no legal liability whatsoever arising from or connected to, the accuracy, reliability, currency or completeness of any material contained in this resource or on any linked site. References to other organisations or websites are inserted for convenience and do not constitute endorsement.



Important note

This resource is intended as a guide only. It should be adapted for every online safety incident and individual involved. Staff members who are unsure of what to do should seek advice from their school principal, school leadership, wellbeing or online safety staff or a senior/supervising colleague.

Every incident response should be consistent with, and informed by, relevant legislation as well as education department or sector policies and procedures.

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.



Assessment tool

This tool is intended only as a guide.

It should be adapted to each online safety incident and the individuals involved. Responses may need to be escalated or de-escalated depending on the situation or new information coming to hand.

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	Rating
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.	
<ul style="list-style-type: none"> • First time and instigator is likely to stop. • Is a contained incident between two people. 	1
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • Has happened many times before. • Instigator unlikely to stop. • Is part of a wider situation involving a number of students/parents/others. 	3

Impact	Rating
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.	
<ul style="list-style-type: none"> • Target appears to be coping well. • Target has a supportive peer group and/or family. • Target can manage with minimal support. 	0
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • Target has identified vulnerabilities. • Target needs ongoing support from school and/or specialist support. 	2
<ul style="list-style-type: none"> • 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](#)

Responding

In responding to incidents, refer to eSafety's [Quick reference guides for online safety incidents](#), and all relevant legislation and sector/school policies and procedures.

eSafety's [Guide to responding to serious online safety incidents](#) and [Guide to dealing with explicit images in school](#) can also help schools identify a suitable response.

Examples of online incident assessments

Important note

The following examples are intended as a guide only. The individual circumstances of online incidents will vary and incidents that appear similar may differ in their impact and seriousness.

Example 1

A student (the instigator) makes a meme about another student (the target) and posts it in a private social media group chat. The targeted student, who has been mocked in the group chat before, told the instigator to delete the meme and reported the incident to a teacher.

Category	Incident type	Rating
Behaviour	Meme post.	1
Frequency	Has happened occasionally as part of a friendship group situation.	2
Impact	Target has indicated that they are coping well with the situation.	0
Total	Mild — the incident can likely be managed by the student. Minimal teacher intervention may be needed to offer support, if the student has already have strategies and can respond appropriately.	3

Example 2

A student (the target) receives a text message from another student (the instigator) that shows a video of someone being punched at a nearby school. The instigator sent the message as a joke, but as the target has been physically bullied in the past, it raises his anxiety and makes him feel threatened and unsafe.

Category	Incident type	Rating
Behaviour	Sharing violent videos.	2
Frequency	First time. Instigator is likely to stop. It is contained between two people.	1
Impact	Significant physical, psychological or emotional impact on target.	3
Total	Serious — the impact is rated as 3, therefore the incident is rated serious at a minimum.	6

Example 3

A student (the target) has received sexually suggestive messages from someone she chats with online. The contact asks her to share nude images of herself which makes her feel uncomfortable. She thought she was chatting with someone she knows at a nearby school, so she confronts them but is met with denial. She wonders if it might be a stranger impersonating another student, but she isn't certain. She feels unsafe and scared.

Category	Incident type	Rating
Behaviour	Online grooming or sharing inappropriate sexualised messages.	3
Frequency	Has happened occasionally and/or has occurred via multiple platforms/mediums.	2
Impact	Target has identified vulnerabilities and the incident is having a significant emotional impact on her.	3
Total	Severe — the behaviour could be classified as sharing inappropriate sexualised messages and/or grooming. In this case, the category with the highest rating should be chosen.	8

Quick reference guides for responding to online safety incidents

eSafety Toolkit for Schools

Creating safer online environments



This resource includes a series of quick reference guides for responding to online safety incidents. It can be used with eSafety's [Online incident assessment tool](#). For further information or support, refer to eSafety's [Guide for responding to serious online safety incidents](#) and [Guide to responding to the sharing of explicit material](#), or refer to education department or sector policies and procedures.

Disclaimer: This material is general in nature. It is made available on the understanding that the Commonwealth is not engaged in rendering professional advice. Before relying on the material in any matter, you should carefully evaluate its accuracy, currency, completeness and relevance for your purposes and should obtain any appropriate professional advice relevant to your particular circumstances. The Commonwealth does not guarantee, and accepts no legal liability whatsoever arising from or connected to, the accuracy, reliability, currency or completeness of any material contained in this resource or on any linked site. References to other organisations or websites are inserted for convenience and do not constitute endorsement.



eSafety's Quick reference guide for responding to **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 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.

eSafety's Quick reference guide for responding to 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 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 existing 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.

eSafety's Quick reference guide for responding to **serious** 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.
- 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 — refer to eSafety's [Guide to responding to the sharing of explicit images](#).
- For non-explicit material, where possible, take screenshots or record URLs.
- 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 (e.g. 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 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 existing policies and procedures following the incident.
- Debrief with staff, students and parents/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.

eSafety's Quick reference guide for responding to **severe** 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.
- 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 — refer to eSafety's [Guide to responding to the sharing of explicit images](#).
- For non-explicit material, where possible, take screenshots or record URLs.
- Check state, territory or school policies. 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 students' 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, if required.
- Assess whether school-wide communication is appropriate.



Remove 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 authorisation.
- 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 processes.
- Complete a [Post-incident checklist](#).
- Review existing policies and procedures following the incident.
- Debrief with staff, students and parents/carers, where appropriate.



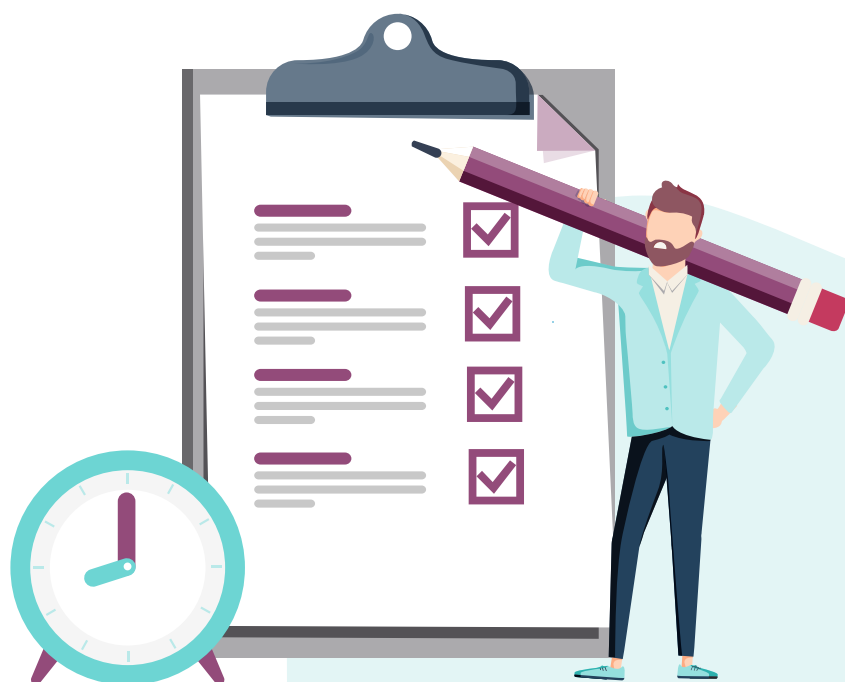
Monitor

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

Post-incident checklist

eSafety Toolkit for Schools

Creating safer online environments



This resource provides a series of guiding questions to help schools to assess incident responses, as well as providing suggestions for improved practice. Schools are encouraged to undertake post-incident reviews after any online safety incident and have processes in place to respond to ongoing issues. The type of review will depend on the severity and impact of the incident.

The National Office for Child Safety has developed a [complaint handling guide](#) which provides advice about how to develop, implement and maintain a complaint-handling system. The guide's approach prioritises child safety and promotes the right of children and young people to have a voice in decisions that affect them.

Disclaimer: This material is general in nature. It is made available on the understanding that the Commonwealth is not engaged in rendering professional advice. Before relying on the material in any matter, you should carefully evaluate its accuracy, currency, completeness and relevance for your purposes and should obtain any appropriate professional advice relevant to your particular circumstances. The Commonwealth does not guarantee, and accepts no legal liability whatsoever arising from or connected to, the accuracy, reliability, currency or completeness of any material contained in this resource or on any linked site. References to other organisations or websites are inserted for convenience and do not constitute endorsement.



Post incident checklist	Yes
Immediate response	
<p>1. Did the students involved in the incident know who to ask for advice and/or know how to report the incident?</p> <ul style="list-style-type: none"> 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. 	<input type="checkbox"/>
<p>2. Did the staff member/s responding to the incident try to understand the context to accurately assess its severity and impact?</p> <ul style="list-style-type: none"> 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. 	<input type="checkbox"/>
Supporting wellbeing	
<p>3. Was support provided to all students involved in the incident (e.g. the target, instigator and bystanders)?</p> <ul style="list-style-type: none"> 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. 	<input type="checkbox"/>
<p>4. Have wellbeing checks been scheduled with all students involved in the incident (i.e. target, instigator and bystanders)?</p> <ul style="list-style-type: none"> 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. 	<input type="checkbox"/>

Post incident checklist	Yes
Supporting wellbeing (continued)	
<p>5. Were all parties involved in the incident — target, instigator, bystanders, parents/carers and staff — debriefed and made aware of the resolution?</p> <ul style="list-style-type: none"> • 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 and help develop their sense of belonging 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. 	<input type="checkbox"/>
External involvement	
<p>6. If the incident involved harmful content circulating online, was the content removed?</p> <ul style="list-style-type: none"> • 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. 	<input type="checkbox"/>
<p>7. If there was media coverage of the incident, was the situation handled in a way that supported student safety and wellbeing?</p> <ul style="list-style-type: none"> • 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. 	<input type="checkbox"/>
<p>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?</p> <ul style="list-style-type: none"> • 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. <p>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.</p>	<input type="checkbox"/>

Post incident checklist	Yes
Finalising the response	
<p>9. Was a record of the incident collected and stored in a safe and secure location?</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. 	<input type="checkbox"/>
<p>10. Has the inappropriate behaviour stopped?</p> <ul style="list-style-type: none"> 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. Reflect on previous strategies that were used to address recurring issues. Identify what did/didn't work and discuss the strategies the school will implement to proactively address unresolved issues with parents/carers. 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. 	<input type="checkbox"/>
<p>11. Are procedural or policy changes required to prevent this issue from recurring?</p> <ul style="list-style-type: none"> 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. 	<input type="checkbox"/>