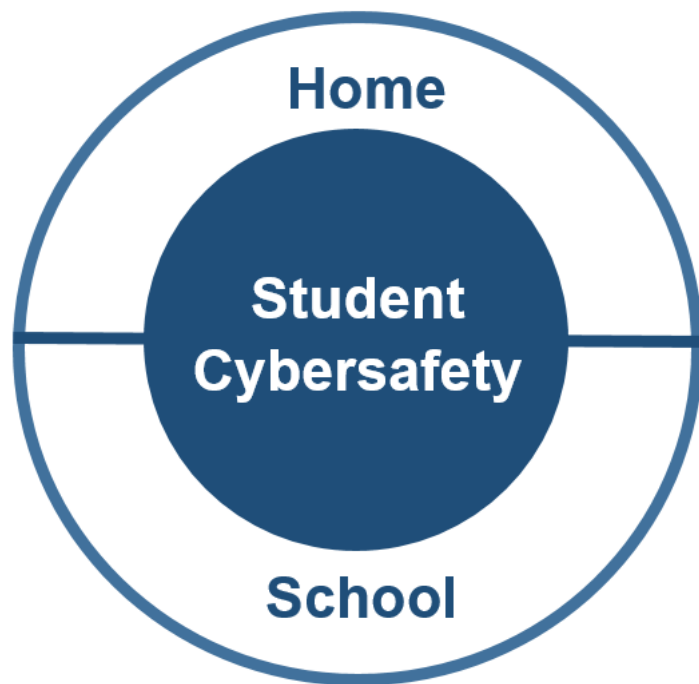


EHSS Cybersafety

Parent Guide



**Working together to
protect our students**



EHSS Cybersafety

Cybersafety Belief Statement

Responsibilities

Eatons Hill State School Cybersafety Belief Statement

The growing prevalence of digital technologies in everyday life is having a significant impact on how students interact and develop. Mobile devices and other technologies provide our students with wonderful opportunities to learn, be creative and socialise, and can provide a positive and enriching experience that is rewarding. However, just as with face-to-face interactions, sometimes bullying and harassment can occur, and just as in the real world, safety measures need to be in place. Cybersafety at Eatons Hill State School is a partnership between the school, families and students. Through shared responsibility and support our students can engage in the digital world in a positive and productive manner.

Leadership's Responsibilities

- Facilitate cybersafety sessions.
- Facilitate teacher development and collaboration on cybersafety.
- Maintain ongoing communication and information sharing with parents.
- Monitoring of any cybersafety updates.
- Monitor the management of cybersafety incidents and ensure ongoing monitoring of cybersafety situations.

Teacher's Responsibilities

- Promote positive cybersafety practices and actively engage with relevant aspects of the curriculum that explore cybersafety.
- Reinforcing cybersafety messages.
- Engage in professional development and collaboration on cybersafety.
- Establish effective routines and practices that support cybersafety practices.
- Communicate with leadership, parents and students about any cybersafety concerns.
- Manage cybersafety incidences in alignment with school policies and communicate measures to be taken with their Deputy Principal
- Retain any evidence of cybersafety concerns.

Parent's Responsibilities

- Promptly communicate with the teacher about any cybersafety concerns.
- Monitor the use of the iPad outside school hours.
- Perform regular random checks of your child's iPad – in particular the search history and online communication.
- Frequently communicate with your child about their cybersafety.
- Ensure only age appropriate apps and content are on your child's device.
- Share with the school any evidence collected relating to cybersafety concerns

Student's Responsibilities

- Use the iPad only when under direct supervision of a teacher or parent.
- Use the iPad in accordance with the school's BYOD iPad Program Student Participation Agreement, iPad Acceptable Use Policy and Guidelines and Responsible Behaviour Plan.
- Promptly communicate with parents and teachers any cybersafety concerns.
- Keep any evidence of cybersafety concerns.



EHSS Cybersafety

EHSS Cybersafety Commitment

Eatons Hill State School Cybersafety Commitments

- Consistent staff supervision while students are using devices - this is the best practice when supporting student safety online.
- Filters are used on all internet accessed through the school to reduce the chance of student access to inappropriate content.
- Cybersafety is embedded in curriculum delivery through the Digital Technologies learning area.
- iPad Boot Camp - when students move into the BYO iPad program in year two they complete rigorous training in appropriate iPad usage and cybersafety.
- Cybersafety is managed through our Responsible Behaviour Plan.
- Ongoing professional development for teachers and support staff on managing cybersafety.
- Leadership team facilitates a cybersafety parent information session.
- The Tech team is available to offer support for cybersafety issues for staff, parents and students.
- An established ICT committee that manages the cybersafety program at Eatons Hill State School.

School Contacts

Who to contact if you have a cybersafety concerns:

Classroom
Teacher

- If you have concerns about cybersafety please contact your child's class teacher immediately.

Deputy
Principal

- Please share any supporting evidence to ensure that they have a clear understanding of the problem.

Principal

- If you have not resolved the concern with the classroom teacher please contact the relevant Deputy Principal and if necessary the Principal.



EHSS Cybersafety

Tips to keep your child safe when they are online

Practical ways to support your child using their iPad safely:

- Remind your child that content can be posted instantaneously, the downfall is that they can potentially post something without thinking about the ramifications.
- Educate your child about appropriate online behaviour and the need for respectful communication with other users.
- Keep an eye on what your child is doing online.
- Set clear rules about what sites and activities they are allowed to access.
- Use family sharing and screen time to limit their use and monitor/restrict the sites they visit.
- Discuss a plan with your child about how to address any cybersafety issues that may arise.



EHSS Cybersafety

Practices in the home that promote cybersafety

Safe settings on the iPad & Internet filtering at home



Practices in the home that promote cybersafety

There are a range of practices that you can do at home that can help to promote cybersafety.

- Introduce a communal charging station—this helps to bring the iPads out of your child's room at night.
- Set screen time limits for non-education activities and enable parental controls.
- Encourage open conversations with your child about being online. It is important to encourage your child to have a safe adult to talk to about cybersafety issues.
- Talk with your child on how to block, unfriend and report inappropriate online behaviour.
- Teach your child to screen shot so they can capture cyber bullying/ inappropriate use.
- Create clear and agreed on rules about iPad usage.
- Promote positive bystander behaviour and the importance of speaking up for others.
- Ensure that your child knows their online friends in the real world first.
- Teach your child to think before sharing: is it true, useful and positive?

Safe settings on the iPad

There are a range of ways you can set up your child's iPad to improve its security. Utilising Family Sharing and Screen Time will allow for you to monitor and manage what your child accesses and when they can use certain apps. It is important to consider the location setting you have on the iPad. Below are links to support documents that will step you through setting up your iPad.

- Family sharing
<https://support.apple.com/en-au/HT201060>
- Screen time
<https://support.apple.com/en-au/HT208982>
- Location settings: consider disabling
<https://support.apple.com/en-au/HT207092>

Internet filtering at home

When your child connects their iPad to the school network, the Education Department's filtering system is designed to assist in protecting them from malicious web content and inappropriate websites. To help protect your child when they return to your home internet connection, it is recommended you install internet filtering. Parental supervision is the best method for protecting your child from inappropriate content. Supervising your child also helps you to identify possible issues as well as identifying the appropriate times to speak with them on different topics such as the dangers of sharing photos. The eSafety Commissioner website offers advice on home filtering and links to a range of recommended systems for families.

<https://www.esafety.gov.au/parents/skills-advice/taming-technology>

EHSS Cybersafety

Social Media, Passwords & Privacy

Social Media

- It is important as a parent to be aware of which social media apps/sites your child is accessing.
- Join your child as a friend/follower on your social media accounts.
- Openly talk with your child about their use of social media.
- Only allow your child to join different social media sites when they meet the age requirements.
- Using Screentime will ensure that your child requires parental permission to access particular websites and install all apps including social media apps.

Passwords

- Teach your child how to create a strong password. Passwords should feature a combination of upper and lower case letters, numbers and symbols.
- Make sure they keep their passwords to themselves and have a routine for changing/updating them.

Privacy

- Help your child to regularly update their privacy settings. Make sure their profile is private and only accessible by people they know personally.
- Limit their personal details shared online - protect their digital footprint.
- Use an avatar for their profile picture or share a photo that doesn't show their face.
- Encourage your child to use a nickname.
- Turn off location settings to ensure that their location is not shared.



EHSS Cybersafety

External contacts, links for reporting & additional resources

Please be aware that not all children report when they are harassed or feel threatened on-line to their parents because they fear that their ability to communicate with their peers will be removed. It is important that they are aware of the other avenues available to them including the School Guidance Officer, Chaplain and other services.

External Contacts

- Lifeline - phone 13 11 14
- Kids Helpline - phone 1800 551 800 for free and confidential counselling for young people aged 5-25
- Parentline - phone 1300 301 300 for support, counselling and parent education
- Office of the eSafety Commissioner – parents and carers
<https://www.esafety.gov.au/parents>

Common links for reporting inappropriate social media content:

- Facebook - <https://www.facebook.com/help/>
- Instagram - <https://help.instagram.com/>
- Google (including YouTube) - <https://support.google.com/>
- Twitter - <https://help.twitter.com/en>
- Snapchat - <https://support.snapchat.com/en-US>
- Tik Tok - <https://support.tiktok.com/en/privacy-safety/report-inappropriate-content-en>

Additional resources

- eSafety's Parents page— www.esafety.gov.au/parents learn about what children do online and how you can encourage them to be positive digital citizens at different ages.
- Stay Smart Online— www.staysmartonline.gov.au/ read about how to protect personal and financial information.
- ThinkUKnow Parents Portal — www.thinkuknow.org.au/ contains information about technologies that are popular with kids and advice about app safety.
- Bullying. No way!— <https://bullyingnoway.gov.au/> provides great information about bullying, harassment, discrimination and violence in schools.

